

AppWorks™
Installation Guide for
Windows
Release 16.7

This documentation has been created for software version 16.7.

It is also valid for subsequent software versions as long as no new document version is shipped with the product or is published at <https://knowledge.opentext.com>.

Open Text Corporation

275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Tel: +1-519-888-7111

Toll Free Canada/USA: 1-800-499-6544 | International: +800-4996-5440

Fax: +1-519-888-0677

Support: <https://support.opentext.com>

For more information, visit <http://www.opentext.com>

Copyright © 2019 Open Text. All Rights Reserved.

Trademarks owned by Open Text.

One or more patents may cover this product. For more information, please visit <https://www.opentext.com/patents>

Disclaimer

No Warranties and Limitation of Liability

Every effort has been made to ensure the accuracy of the features and techniques presented in this publication. However, Open Text Corporation and its affiliates accept no responsibility and offer no warranty whether expressed or implied, for the accuracy of this publication.

Last updated: 10/17/2019

Table of Contents

Chapter 1 Introduction	7
Product components	7
Audience	8
Installation overview	8
Chapter 2 System requirements	10
Environment support	11
Server requirements	11
Client requirements	12
Chapter 3 Installation checklists	13
AppWorks installation considerations	14
Pre-installation checklist	14
Installation and configuration checklist	15
Installation worksheet	17
Chapter 4 Getting started	20
Downloading the installation bundle	20
Chapter 5 Configuring third-party software	22
Configuring Java	22
Configuring environment variable after installing Java	23
Configuring a database	24
Prerequisites	25
Prerequisites for an existing database	26
Prerequisites for an existing MS SQL server database	26
Prerequisites for an existing Oracle database	26
Prerequisites for an existing PostgreSQL database	28
Post-installation configuration for PostgreSQL	28
Configuring Tomcat	28

Configuring Apache Tomcat properties	29
Editing Tomcat connector definition	29
Configuring TomEE	30
Downloading TomEE	30
Creating a TomEE user	30
Granting TomEE access to the installation directory	31
Adding a default value environment variable	32
Installing the TomEE service	33
Updating the TomEE configuration	34
Configuring JDBC driver for TomEE	34
Configuring for MS SQL	34
Configuring for Oracle	35
Configuring for PostgreSQL	36
Configuring TomEE ports	36
Chapter 6 Initiating AppWorks installation	39
Chapter 7 Installing AppWorks Platform	43
Installing CARS	44
Installing AppWorks Platform baseline	46
Deploying AppWorks Platform applications	51
Verifying AppWorks Platform installation	54
Hardening AppWorks Platform security	54
Chapter 8 Installing OpenText Directory Services	55
Installing OpenText Directory Services	55
Verifying the OTDS installation	58
Chapter 9 Configuring OpenText Directory Services	59
Configuring OTDS for AppWorks Platform	59
Adding an OTDS partition	59
Adding an OTDS user	60
Configuring AppWorks Platform for OTDS authentication	61
Creating a resource for AppWorks Platform	62
Configuring AppWorks Platform for OTDS authentication	65
AppWorks Platform OTDS authentication	65
AppWorks Platform trusted sites	66

Configuring OTDS authentication for an organization	67
Creating a user to push users and groups into AppWorks Platform	68
Creating an organization-specific partition for groups and roles	69
Creating an organization-specific resource for AppWorks Platform in OTDS	69
Linking the organization-specific partition to the organization-specific resource ..	72
Synchronizing roles	73
Creating a process administrator user	73
Managing users and group membership for a specific organization	74
Consolidating a resource	75
Verifying the configuration	76
Disabling the authentication handler	76
Chapter 10 Installing and configuring Process Intelligence	77
Configuring the databases	79
Verifying the installation	80
Integrating Process Intelligence with AppWorks Platform	82
Configuring a distribution	83
Configuring a publisher	83
Configuring a subscriber	88
Disabling publishing and distribution	89
Running database scripts	91
Integrating Process Intelligence with iHub	91
Chapter 11 Installing and configuring Brava	92
Installing Brava Enterprise	93
Configuring Brava Viewer with AppWorks Platform	95
Appendix A High availability	96
AppWorks high availability architecture	96
Identifying high-availability components	98
AppWorks products	98
Other components	99
Configuring AppWorks high availability	99
Configuring AppWorks Platform	100
Configuring AppWorks web gateway	101
Configuring Process Intelligence	102

Configuring OpenText Directory Services	104
High availability best practices	104
High availability maintenance	105
Adding a new node to the AppWorks cluster	105
Adding AppWorks Platform	106
Removing a node from AppWorks cluster	106
Uninstalling AppWorks Platform	106
Applying AppWorks updates, fixes, or upgrades	106
Validating the high availability configuration	107
Planned and unplanned outage	107
Appendix B Configuring iHub for AppWorks Platform	108
Configuring iHub with HTTPS	108
Configuring system console for iHub	109
Deploying Process Suite RSSE	110
Configuring AppWorks Platform for iHub	112
Integrating Process Intelligence with iHub	113
Appendix C AppWorks Platform REST APIs	114
Invoking AppWorks Platform REST APIs	114
Downloading REST client	114
Configuring REST Client	114
Invoking AppWorks Platform REST APIs	115
Appendix D Configuring IIS	116
Appendix E Upgrading AppWorks	117
Upgrading AppWorks Platform	117
Upgrading OTDS	117
Upgrading Process Intelligence	117
Upgrading Brava	118
Appendix F Troubleshooting	119
General troubleshooting	119
Troubleshooting OTDS	119
Appendix G Configuring online help on a Private Help Server	122
Providing the online help on a local help server (Private Help Server)	122
Configuring AppWorks Platform to use a local help server (Private Help Server) ..	123

Chapter 1

Introduction

AppWorks allows you to design, implement, monitor, and continuously optimize business processes and operations within single or multiple environments.

The AppWorks Installation Guide explains how to install new versions of AppWorks.

Topics include:

- [Product components on page 7](#)
- [Audience on page 8](#)
- [Installation overview on page 8](#)

Product components

The AppWorks installation process makes use of installation wizards of the individual components of AppWorks with some post-installation tasks to integrate all the components. The installation procedure guides you through the individual installation procedure for each core component in the selected sequence.

The following table provides the list of components in AppWorks:

Component	Description
AppWorks Platform	<p>Provides a Business Process Management (BPM) solution organizations can use to design, execute, monitor, change, and continuously optimize their critical business processes and operations.</p> <p>AppWorks Platform comprises:</p> <ul style="list-style-type: none">■ OpenText CARS■ Process engine■ Task and Case management■ Entity runtime■ Connector integration framework
OpenText Directory	<p>Provides a centralized authentication mechanism and user-role management functionality for all the OpenText Products in the bundle.</p>

Component	Description
Services (OTDS)	To enable single sign on for the users across these products, integrate your user and role database such as Active Directory or LDAP, with OTDS and register the OpenText products as resources to centralize the users.
Process Intelligence	Analyzes data to deliver insight and operational status information for AppWorks. It receives information from a business process, transforms it into useful business intelligence, and reflects it in business intelligence reports.
Brava Viewer	Enables you to view documents, images, CAD files and so on quickly and easily within and across the enterprise. It is the default document viewer for documents attached to case models, processes, entity-based applications in AppWorks Platform.
Analytics	Reporting tool that enables you to analyze large volumes of data you have received or sent. It includes: <ul style="list-style-type: none">■ System Console■ Information Hub■ Analytics Designer Note: This component is not provided as part of the AppWorks bundle. To use the reporting capabilities provided by OpenText Analytics, download and install the software from My Support and integrate it with AppWorks.
Gateway	Enables you to efficiently deploy all the APIs, Web services, and mobile applications you build with AppWorks. It provides single sign-on, centralized application and audience management as well as seamless application updating capabilities and enables access to all the capabilities of OpenText Enterprise Information Management (EIM). Since apps are independent from one another, you can allow access to specific applications for specific user audiences.

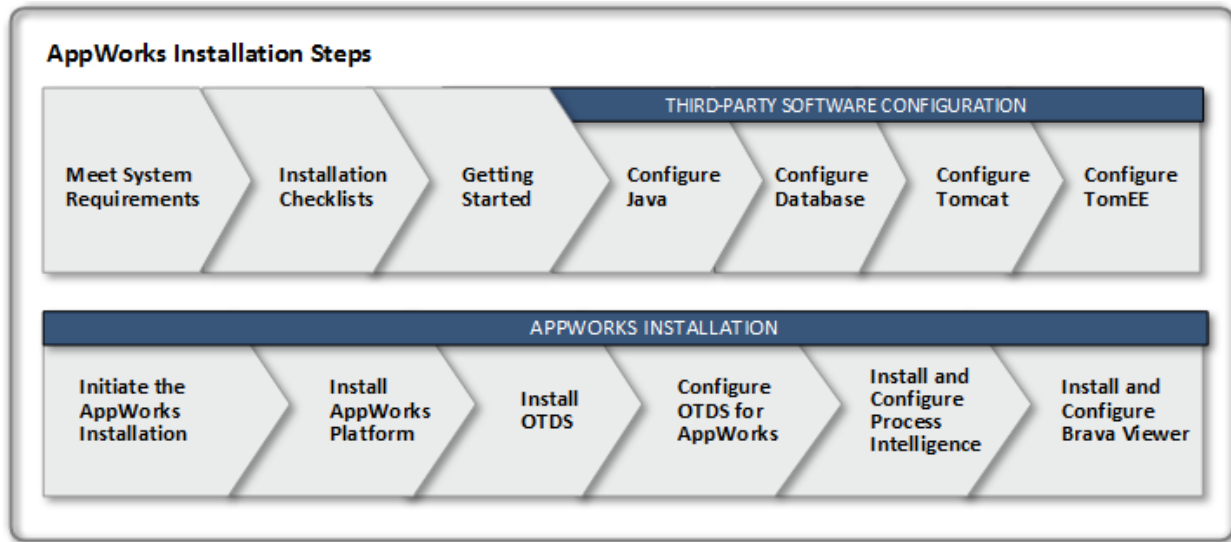
Audience

The AppWorks Installation Guide is for system administrators or users with administrative privileges who are responsible for installing AppWorks. It is highly recommended that users have a good knowledge of configuring databases, configuring OpenText Directory Services (OTDS), and administering Web servers like TomEE.

Installation overview

Installing AppWorks requires the installation and deployment of a number of components. The following illustration provides a high-level overview of the steps required for installing

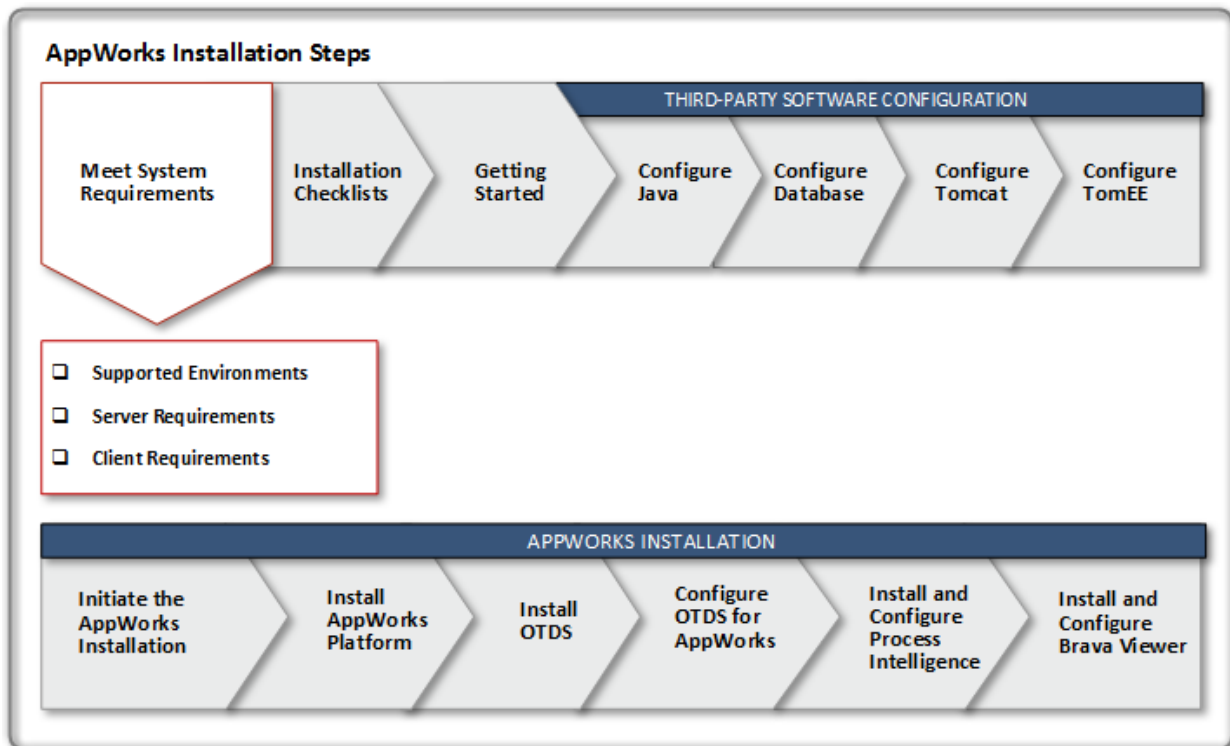
AppWorks.



Chapter 2

System requirements

Before installing AppWorks, ensure that all hardware, software, and database requirements are met. Obtain the necessary configuration information before starting the installation.



Important: AppWorks components can be installed on the same server. However, for optimal utilization of resources, the database server and OTDS can be installed on separate servers. Additionally, it is also recommended that Content Server and Process Intelligence be deployed on separate servers due to their requirements.

The following sections list the minimum hardware and software requirements for installing AppWorks.

System requirement information includes:

- [Environment support on page 11](#)
- [Server requirements on page 11](#)
- [Client requirements on page 12](#)

Environment support

AppWorks bundle comprises multiple products that are supported through various combinations of operating systems, databases, and other software products. It is recommended that you go through the relevant environment support documents on [My Support](#) as specified below :

- AppWorks Platform - See the AppWorks Platform environment support guide for a comprehensive list of supported environments for AppWorks Platform.
- OTDS - See the Supported environments and compatibility section in the Release Notes of the corresponding version.
- Process Intelligence - See the Environment Support section in the Process Intelligence Installation and Configuration guide of the corresponding version.
- Brava Viewer - See the Supported environments and compatibility section in the Release Notes of the corresponding version.
- AppWorks Gateway - See the Supported environments and compatibility section in the Release Notes of the corresponding version at Developer.opentext.com.

Server requirements

The following table lists the minimum server requirements for hosting AppWorks services.

Recommendation: Separate servers for each component

Hardware	Processor	Processor speed	RAM	Disk space
AppWorks Platform	Quad core x64 architecture	2 GHz or faster	Use one of the following: 16 GB for production environments 12 GB for development or test environments This memory requirement is for AppWorks Platform.	2 GB free disk space. For installation purposes only.
Process Intelligence	Intel Pentium IV processor Recommended: Core 2 Duo CPU or better.	2.5 GHz	4 GB or higher	The Analysis Engine, Server Administration, and Integration Service computers, depending on system sizing, may require 20-40 GB or more of disk space.

Hardware	Processor	Processor speed	RAM	Disk space
Brava Enterprise	Pentium 3 (or equivalent)	1.5GHZ with 1024 MB of RAM is recommended	1024MB (1536MB or higher recommended)	<ul style="list-style-type: none"> - 70MB available hard disk space is required for Job Processor and all installed files - At least 500MB (depending on amount and size of original files) of hard disk space is required for temporary files created during the processing of requests - Additional disk space is required for temporary files during publishing. Space requirement varies with number and complexity of documents served – we recommend at least 5GB of temporary disk space on the C: drive for processing of files through the IGC Writer.

Client requirements

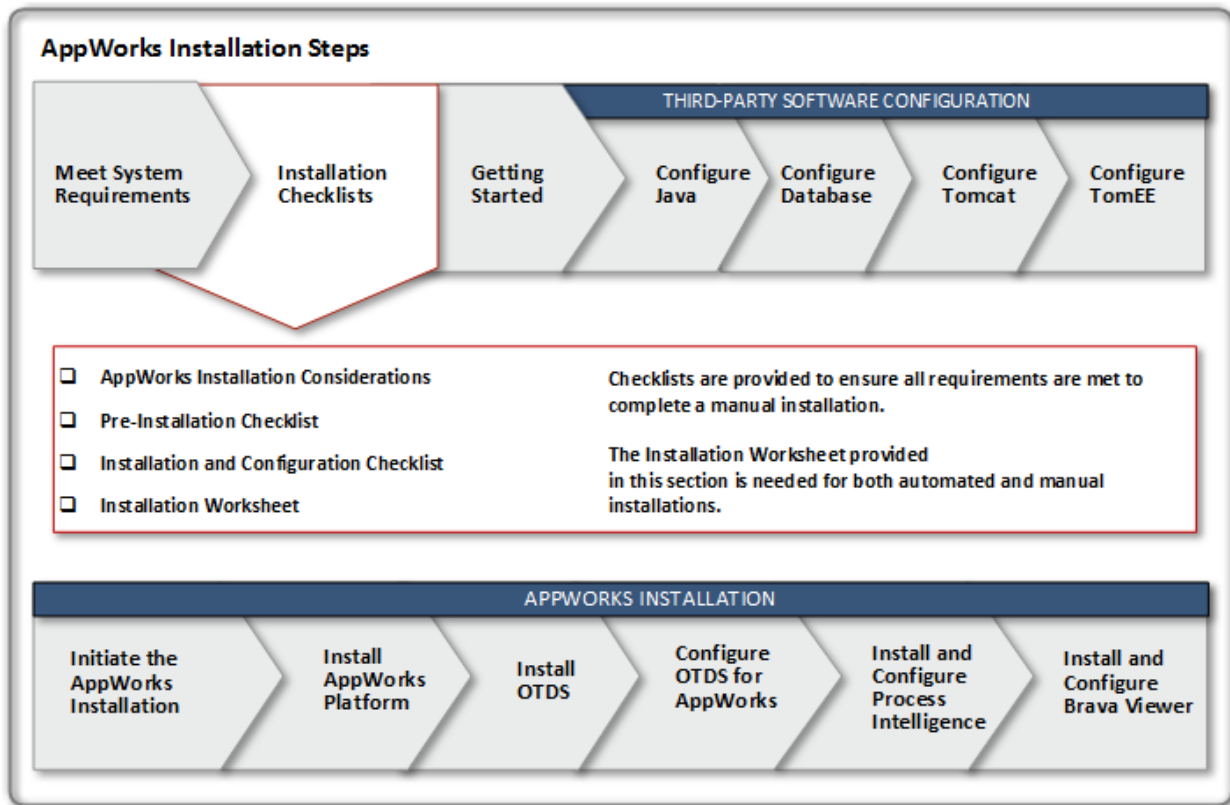
The following table lists the minimum hardware requirements to access AppWorks services installed on a server:

Hardware	Specification
Processor	Dual core
Processor speed	2 GHz or faster
RAM	8 GB
Monitor resolution	1280x1024
Color depth	32 bits or higher
Monitor DPI	96

Chapter 3

Installation checklists

This section provides a high-level overview of the steps required for a successful installation of AppWorks.



Topics include:

- [AppWorks installation considerations on page 14](#)
- [Pre-installation checklist on page 14](#)
- [Installation and configuration checklist on page 15](#)
- [Installation worksheet on page 17](#)

AppWorks installation considerations

Important: The installation instructions and related screenshots of the products, such as AppWorks Platform, OpenText Directory Services, Process Intelligence, Brava, and Information Hub, provided in this guide meet the minimal installation requirements. For instructions on advanced installation requirements, see the installation guide of the corresponding product on [My Support](#).

Review the following notes carefully before starting the installation.

- AppWorks Platform, when installed as part of the AppWorks bundled installation, can be installed on the same computer as the other AppWorks components or on a different computer. However, as the AppWorks components are data and resource-intensive, it is highly recommended to install each of the following components on a separate server:
 - AppWorks Platform
 - Process Intelligence
 - Brava Viewer
 - Information Hub

Note: OTDS can be installed on the server hosting AppWorks Platform.

- The AppWorks components use Web servers such as TomEE, Tomcat, and IIS. Installing two or more components on the same server might result in port conflicts. Therefore, identify the correct port for each component to prevent cross-domain issues while working in AppWorks.
- Multiple instances of AppWorks Platform can be installed on the same computer. Each instance is identified with a unique name and is independent of other instances.

Pre-installation checklist

Before beginning the installation process, do the following:

	Task	Description
<input type="checkbox"/>	Meet all system requirements	System requirements on page 10
<input type="checkbox"/>	Set administrative privileges	Grant administrative privileges on the computer where the installations are to be performed for the user performing the install and that this user has WRITE privileges.
<input type="checkbox"/>	Verify AppWorks installation environments	Verify that all computers where AppWorks is to be installed are in the same domain and the administrator has appropriate permissions on the Active Directory.

	Task	Description
<input type="checkbox"/>	Verify the third-party software installations.	<p>Verify if the relevant versions of Java, database, and Web server are installed.</p> <p>See the Environment Support matrix on My Support for the list of supported environments for AppWorks.</p> <p>If not installed, see the installation guide for the corresponding software vendor for instructions on installing the required software.</p>
<input type="checkbox"/>	Obtain installation information	<p>Print and complete the Installation worksheet on page 17 before you begin installation. This worksheet is used throughout the installation process.</p> <p>Additionally, use it to track information generated during the installation, which is needed later in the process.</p> <p>Note: Open a text file editor, such as Notepad, to record information generated during the installation. You can reuse this information during the install process.</p>
<input type="checkbox"/>	Download the installation zip file bundle to the AppWorks installation folder <extracted_installdir>	Getting started on page 20

Installation and configuration checklist

The following checklist provides the sequence of steps required to install AppWorks.

	Task	See
<input type="checkbox"/>	Complete pre-installation checklist	Installation checklists on page 13
<input type="checkbox"/>	Configure the third-party software for AppWorks. Note: For supported versions, see the AppWorks Supported Environments guide in OpenText MySupport .	Configuring third-party software on page 22
	<input type="checkbox"/> Configure Java	Configuring Java on page 22

	Task	See
	<ul style="list-style-type: none"> ■ Configure Database 	Configuring a database on page 24
	<ul style="list-style-type: none"> ■ Configure TomEE 	Configuring TomEE on page 30
	<ul style="list-style-type: none"> ■ Configure Tomcat (Required only if you use OTDS and have installed Tomcat)	Configuring Tomcat on page 28
<input type="checkbox"/>	Initiate the AppWorks installation	Initiating AppWorks installation on page 39
<input type="checkbox"/>	Install CARS	Installing CARS on page 44
<input type="checkbox"/>	Install AppWorks Platform	Installing AppWorks Platform on page 43
	<ul style="list-style-type: none"> ■ Install AppWorks Platform baseline ■ Install AppWorks Platform applications 	Installing AppWorks Platform baseline on page 46 Deploying AppWorks Platform applications on page 51
<input type="checkbox"/>	Install OpenText Directory Services (OTDS) (Required for Identity Package and if OTDS is used as the authentication mechanism)	Installing OpenText Directory Services on page 55
<input type="checkbox"/>	Configure OTDS	Configuring OpenText Directory Services on page 59
<input type="checkbox"/>	Install Process Intelligence	Installing and configuring Process Intelligence on page 77
<input type="checkbox"/>	Integrate Process Intelligence with AppWorks Platform	Integrating Process Intelligence with AppWorks Platform on page 82
<input type="checkbox"/>	Install Brava Viewer	Installing and configuring Brava on page 92
<input type="checkbox"/>	Configure iHub	Configuring iHub for AppWorks Platform on page 108
	Optional Installations	
<input type="checkbox"/>	Install and configure the REST API client for AppWorks	Invoking AppWorks Platform REST APIs on page 115
<input type="checkbox"/>	Install Analytics	Download OpenText Analytics from My Support . See the corresponding installation and administration guides for instructions on the installation procedures.

Installation worksheet

Print this page and obtain the values for these items before or during the installation process. These values are used in various configuration steps so it is vital that you note these values as you go for a successful installation. All values required to be recorded are identified in the procedures.

Caution: Before you start installing AppWorks Platform, ensure that any user input you provide to the installer does not contain more than one dollar character \$. The installer ignores any content between the dollar characters including the dollar characters.

Recommendation: Open a file in Notepad to copy the values, as some are lengthy numeric ones. This enables you to reuse long strings of information.

	Item	Value
<input type="checkbox"/>	Host server name / ID	
<input type="checkbox"/>	<Extracted_installdir> name (absolute path to where the installation bundle is downloaded and files extracted)	
<input type="checkbox"/>	JDK installation directory	
<input type="checkbox"/>	Absolute path to the JDBC jar file	
<input type="checkbox"/>	Absolute path to x64 folder	
<input type="checkbox"/>	TomEE <ul style="list-style-type: none"> • User ID • Password • Port number Important: Tomcat and TomEE are different and cannot use the same ports. Recommended to use port 81 for TomEE.	
<input type="checkbox"/>	Tomcat <ul style="list-style-type: none"> • Administrator Login ID • Password • Port number 	
<input type="checkbox"/>	OTDS user name and passwords <ul style="list-style-type: none"> • Admin name • Password • User name 	

	Item	Value
	<ul style="list-style-type: none"> • Password 	
<input type="checkbox"/>	CARS <ul style="list-style-type: none"> • Instance name • Port number • User name • Password 	
<input type="checkbox"/>	AppWorks Platform License Information (Usually provided by the sales team) <ul style="list-style-type: none"> • Registered Customer Name • Registered Site Name (available in the Sales materials) • Password for the site, provided by OpenText. 	
<input type="checkbox"/>	AppWorks Platform <ul style="list-style-type: none"> ■ User Name ■ Password 	
<input type="checkbox"/>	AppWorks Platform Resource Identifier (You can save this value in a text editor for later use)	

Additional information on ports

The following table contains the recommended and mandatory port information. If you have to install more than two products on the same server, ensure that you meet the following port requirements:

Component	Recommended port	Mandatory port	Remarks
CARS	6366	No	Can be changed during installation
AppWorks Platform	80 for http or 433 for https. As a best practice, configure TomEE with SSL on 443	No	Can be changed in TomEE configuration. Common alternatives are ports 8080, 8081, 9090 and 8433, 9433, etc.
OTDS	80 for http or 433 for	No	Can be changed in

Component	Recommended port	Mandatory port	Remarks
	https. As a best practice, configure Tomcat with SSL on 443		Tomcat configuration. Common alternatives are ports 8080, 8081, 9090 and 8433, 9433, and so on.
Process Intelligence	80 This is the default port for deploying any web application to IIS.	Yes	No
Brava	8080	No	Can be changed during webserver installation
iHub	See iHub	Yes	No
Tomcat	See OTDS	No	
TomEE	See AppWorks Platform	No	
Database	Varies from database to database SQL Server – 1433 Oracle – 1521 PostgreSQL – 5432	No	Can be configured to a different port during installation of database server
Java JMX RMI port	1099	No	

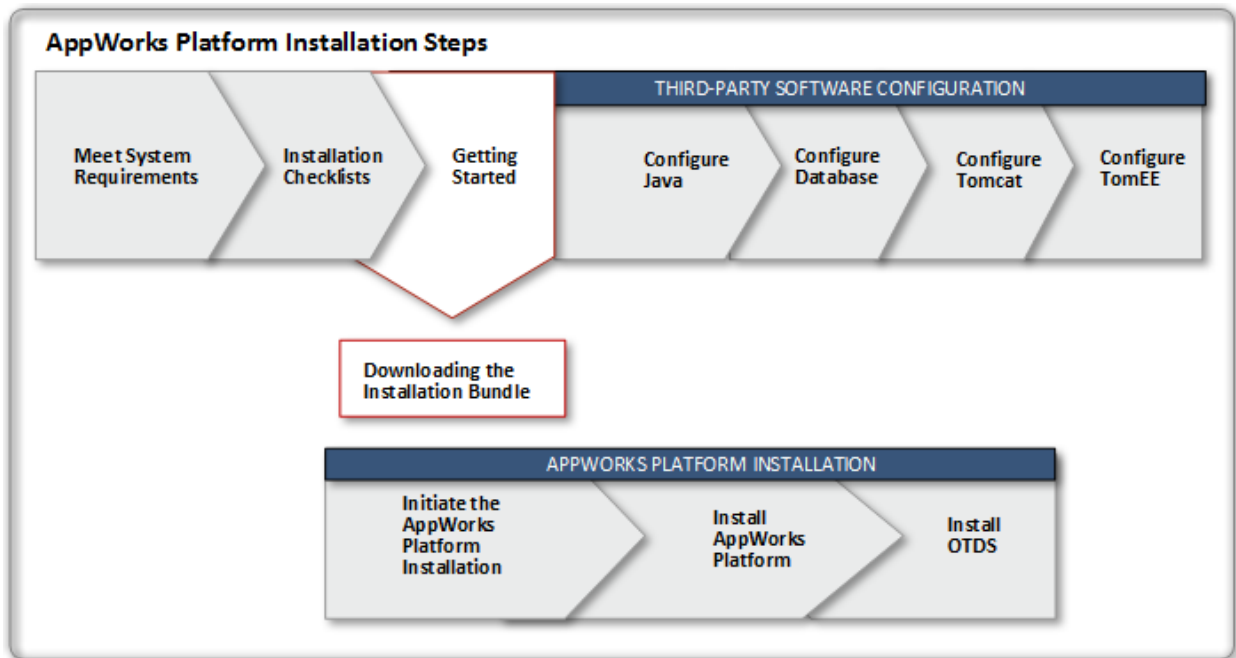
Before you begin:

- If you already have one or more products installed, or if you choose not to install all the components, the installer opens the installation wizard of the selected products one after another.
- Ensure that the installation of the previous product is complete and that the post-installation tasks are done as described in the corresponding product installation and configuration guides.
- For references to the <extracted_installdir> in the guide, see the location where you extracted the content of the AppWorks installer package.

Chapter 4

Getting started

Before proceeding with the AppWorks installation, download the installation bundle from [My Support](#) and then stage the bundle for installation. The bundle contains the installers necessary to initiate an automated installation or a manual installation. Obtain a link to [My Support](#) from your sales representative or the Customer Support department.



Downloading the installation bundle

To download the installation bundle:

1. Create an AppWorks install folder on your desktop.
This is the destination location where the installer zip file is to be copied and referred to as the **<extracted_installdir>**.
2. Access the OpenText Customer Support Knowledge Base Site and navigate to the folder containing the latest AppWorks installer.

3. Copy the installer zip file, `OpenText_AppWorks_16.7.zip`, to the **<extracted_installdir>** just created in Step 1, where, 16.x.x is the current release of the AppWorks software bundle.

Note: Copying the zip file can take a significant amount of time. Configure the third-party software during this time and then extract the zip file.

Chapter 5

Configuring third-party software

AppWorks requires the support of a number of third-party applications. This section provides the special considerations or configurations for implementing these software packages to suit AppWorks requirements.

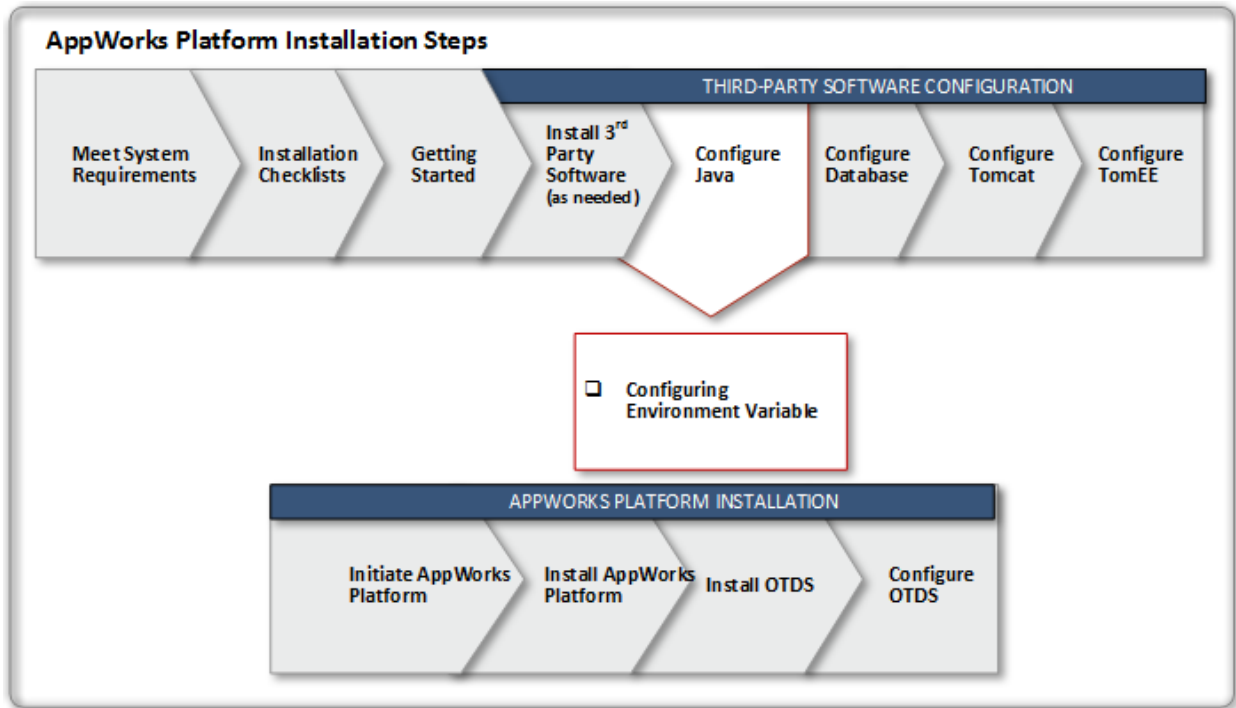
Topic includes:

- [Configuring Java on page 22](#)
- [Configuring a database on page 24](#)
- [Configuring Tomcat on page 28](#)
- [Configuring TomEE on page 30](#)

Note: For supported versions, see the AppWorks Supported Environments guide in [OpenText MySupport](#).

Configuring Java

This section provides instructions for configuring Java as it applies to AppWorks.



Configuring environment variable after installing Java

After you complete the Java installation, configure the environment variable.

Set the `JAVA_HOME` system environment variable to **<JDK_installdir>**.

To configure the environment variable:

1. From the Start menu, select **Run**. Type `sysdm.cpl`, and click **OK**.
The System Properties dialog box opens.
2. Click **Advanced** > **Environment Variables**.
The Environment Variables dialog box opens.
3. Under System variables:
 - Scroll to see whether an existing `JAVA_HOME` variable is available. If one exists, select the `JAVA_HOME` variable, and then click **Edit**.
 - If the `JAVA_HOME` directory does not exist, click **New**.

An Edit or New System Variable dialog box opens.

4. Enter the following information:

Variable name	JAVA_HOME
Variable value	C:\Program Files\Java\jdk11.0.2

5. Click **OK**.

The Environment Variables dialog box refreshes with the updated information.

6. Under System variables, repeat the process for the `Path` variable:

- Scroll to see whether an existing `Path` variable is available. If one exists, select the `Path` variable, and click **Edit**.
- If the `Path` variable does not exist, click **New**.

An Edit New System Variable dialog box opens.

7. Type or modify the `Path` variable with the **Variable value** set with the absolute path to the **bin** folder for the **<JDK_installdir>**.

Note: If the `Path` variable exists, move to the end of the existing variable value and append the following path to this variable value:

`;<JDK_installdir\bin>`

For example:

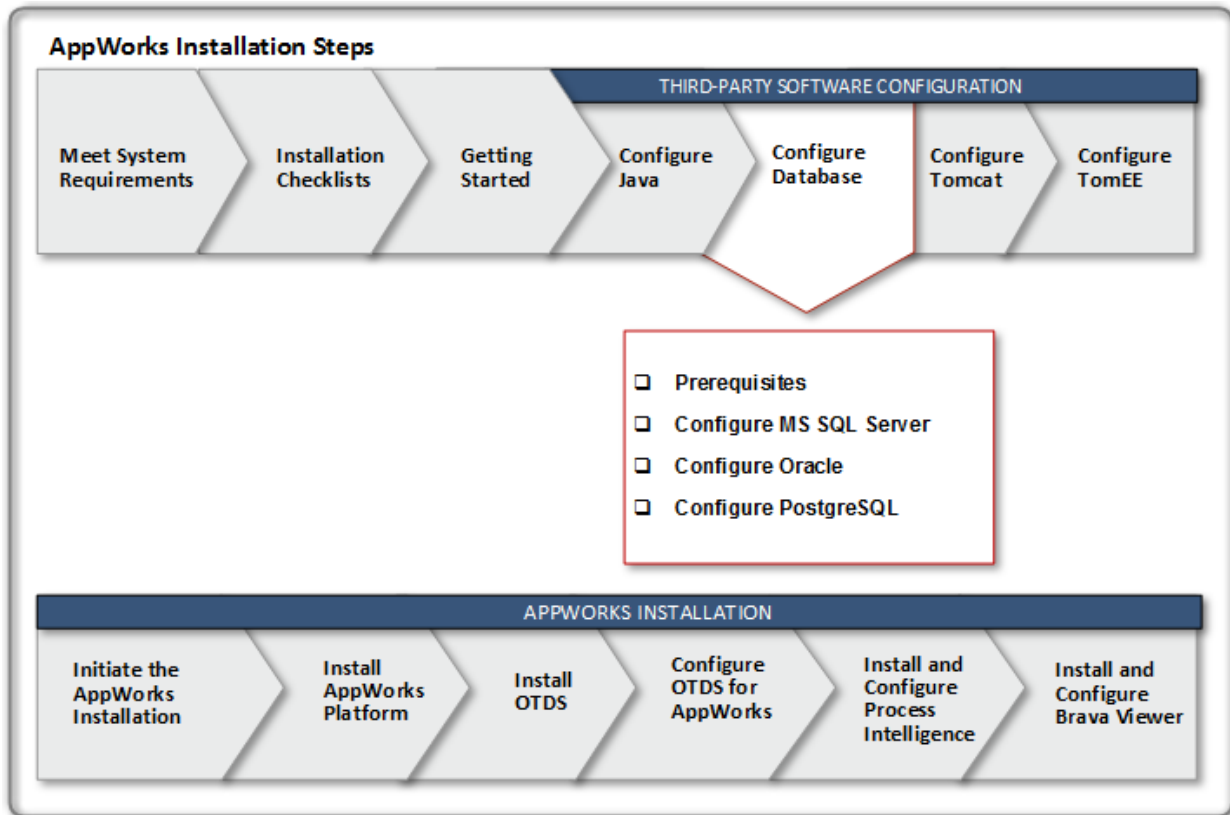
Variable name	Path
Variable value	C:\Windows;C:\Program Files\Java\jdk11.0.2\bin

8. Click **OK** to accept the change, and close the System Variable dialog box.
9. Click **OK** to exit the Environment Variables.
10. Click **OK** again to exit the System Properties dialog box.

Configuring a database

AppWorks supports the following databases:

- MS SQL Server
- Oracle
- PostgreSQL



The following section provides information on the configuration requirements for each database.

Prerequisites

Ensure that your database satisfies the following:

Database naming convention	The database name used for installing AppWorks should not contain '.' (dot character) in the name.
Database size requirements	<p>The initial sizes of a data file in a database and its growth rate impact the performance of database operations. This in turn impacts the performance of AppWorks during design time and runtime.</p> <p>The actual data file size depends upon the volume of transactions. The minimum recommended data file sizes are given below:</p> <p>Production Environment:</p> <ul style="list-style-type: none"> Initial data file size of 5 GB and Auto growth of 1 GB

	<ul style="list-style-type: none"> ■ Log file initial size of 2 GB and Auto growth of 1 GB
	<p>Development Environment:</p> <ul style="list-style-type: none"> ■ Initial data file size of 500 MB and Auto growth of 100 MB ■ Log file initial size of 250 MB and Auto growth of 100 MB ■ If the size of your project is higher than the recommended sizes, allocate higher sizes.

Prerequisites for an existing database

If you are using an existing database to connect to AppWorks, based on your database, you must ensure the following before installing AppWorks. Refer to the appropriate section as it applies to your database:

- [Prerequisites for an existing MS SQL server database on page 26](#)
- [Prerequisites for an existing Oracle database on page 26](#)
- [Prerequisites for an existing PostgreSQL database on page 28](#)

Prerequisites for an existing MS SQL server database

- The AppWorks database is of the same collation as the system database (specifically temporary database (tempdb). This applies to cases where DBA or administrator creates a database and then installs AppWorks using that database. If the database is created during AppWorks installation, the default collation of the server will be used.
- The MS SQL Server user has all the permissions on the database and that the user has `db_owner` role.
- The `READ_COMMITTED_SNAPSHOT` option is set to `true` on the database. Contact DBA for further assistance.
- The MS SQL Server database must be configured to use the `dbo` schema. This is required for the Entity runtime feature in AppWorks.
- The collation name to be used is as follows: `SQL_Latin1_General_CP1_CI_AS`

Note: You need not specify a separate sort order, character set, and collation, as the required characteristics are provided by the collation name.

Prerequisites for an existing Oracle database

- The Oracle user has necessary privileges. AppWorks requires privileges to do the following operations on the schema:
 - `SESSION` - Create/Alter
 - `TABLE` - Create/Alter/Drop
 - `INDEX` - Create/Alter/Drop

- VIEW - Create/Drop
 - PROCEDURE - Create/Alter/Drop/Execute
 - TRIGGER - Create/Alter/Drop
 - SEQUENCE - Create/Alter/Drop
 - DBMS_LOCK - Execute
 - TYPE - Create
- The compression at Oracle database server level is not supported. Therefore, OpenText recommends that you disable compression before performing installation. Contact your database administrator on disabling compression at database server level.
 - Optionally, to enable XA settings, grant the following rights to the user who connects to the database:
 - `Grant select on sys.dba_pending_transactions to <user name>;`
 - `Grant select on sys.pending_trans$ to <user name>;`
 - `Grant select on sys.dba_2pc_pending to <user name>;`
 - `Grant execute on sys.dbms_system to <user name>;`
 - Optionally, to use SSL for Database connectivity with JDBC, you must configure the Oracle service name as TCPS. See Oracle documentation for the procedure.
 - The following parameters and the default values or characteristics are set:
 - NLS_CALENDAR: GREGORIAN
 - NLS_CHARACTERSET: AL32UTF8 for multibyte support
 - NLS_COMP: BINARY
 - NLS_CURRENCY: \$
 - NLS_DATE_FORMAT: DD-MON-RR
 - NLS_DATE_LANGUAGE: AMERICAN
 - NLS_DUAL_CURRENCY: \$
 - NLS_ISO_CURRENCY: AMERICA
 - NLS_LANGUAGE: AMERICAN
 - NLS_LENGTH_SEMANTICS: BYTE
 - NLS_NCHAR_CHARACTERSET: AL16UTF16
 - NLS_NCHAR_CONV_EXCP: FALSE
 - NLS_NUMERIC_CHARACTERS: .,
 - NLS_SORT: BINARY
 - NLS_TERRITORY: AMERICA
 - NLS_TIME_FORMAT: HH.MI.SSXFF AM
 - NLS_TIME_TZ_FORMAT: HH.MI.SSXFF AM TZR

- NLS_TIMESTAMP_FORMAT: DD-MON-RR HH.MI.SSXXF AM
- NLS_TIMESTAMP_TZ_FORMAT: DD-MON-RR HH.MI.SSXXF AM TZR

Prerequisites for an existing PostgreSQL database

- The database has UTF8 character set/encoding.
- The PostgreSQL user has the privileges to perform the following operations on the database:
 - CONNECT
 - CREATE TEMPORARY
 - SELECT
 - INSERT
 - UPDATE
 - DELETE
 - TRUNCATE
 - EXECUTE
 - REFERENCES

Post-installation configuration for PostgreSQL

After installing PostgreSQL, ensure that the relevant jar is added to the /lib folder and set the relevant file controls.

1. From the following link, <https://jdbc.postgresql.org/download.html>, download the relevant jar. For example, postgresql-9.4.1208
2. Copy the postgresql-9.4.1208.jar to the /lib folder of TomEE installation.
3. Edit /opt/PostgreSQL/9.4/data/pg_hba.conf and add the following line under IPV4 local connections:
host all all 0.0.0.0/0 md5
4. Save and close the file.

Configuring Tomcat

Before you begin: You must have the port number provided during the Tomcat installation, as this port number is required for subsequent configurations. Refer to the installation worksheet for the details.

Important: This port number must be different from TomEE as these are two different software components.

Configuring Apache Tomcat properties

The following instructions provide the configuration information needed to set the automatic startup routine and memory pool.

To configure Apache Tomcat properties:

1. Open the Monitor Apache Tomcat tool. Click **All Programs > Apache Tomcat > Monitor Tomcat**.
The Apache Tomcat Properties dialog box opens.
2. If you did not select **Service Startup** when you installed Tomcat, set the Startup type to **Automatic**. On the **General** tab, for Startup type, select **Automatic** and click **Apply**.
3. Click the **Java** tab.
The Java Properties tab opens.
4. Set the **Initial memory pool** to **512**.
5. The Maximum memory pool is the maximum amount of virtual memory that the Tomcat process can use. OpenText recommends that you enter the following value or a greater one as needed:
 - If your number of users is 25,000 or less, enter a value of 1024 MB or more
 - If your number of users is 25,000 to 50,000, enter a value of 2048 MB or more
 - If your number of users is 50,000 to 100,000+, enter a value of 4096 MB or more
6. Click **OK**.

Editing Tomcat connector definition

To edit the connector definition:

1. Navigate to the `<Tomcat_installdir> > conf`, right-click **server.xml** and select **Edit**.
2. Search for the Connector definition line. For example, locate the following lines:

```
<Connector port="8080" protocol="HTTP/1.1"
connectionTimeout="20000"
redirectPort="8443" />
```

Note: The Port number must match the port number defined in the Tomcat installation. Refer to the Installation Worksheet if needed.

4. Add a new attribute called `maxHttpHeaderSize="65536"` at the end of this definition. For example:

```
<Connector port="8080" protocol="HTTP/1.1"
connectionTimeout="20000"
redirectPort="8443" maxHttpHeaderSize="65536" />
```

5. Save and close the file.
6. From the Start menu, select **Run**.
7. Type **services.msc**, and then click **OK**.
The Services window opens.
8. Right-click **Apache Tomcat Service** and select **Start**.

Configuring TomEE

This section provides instructions on configuring TomEE.

Topic includes:

- [Downloading TomEE on page 30](#)
- [Creating a TomEE user on page 30](#)
- [Granting TomEE access to the installation directory on page 31](#)
- [Adding a default value environment variable on page 32](#)
- [Installing the TomEE service on page 33](#)
- [Configuring JDBC driver for TomEE on page 34](#)
- [Configuring TomEE ports on page 36](#)

Downloading TomEE

To download TomEE:

1. Navigate to the Apache TomEE installer: <http://tomee.apache.org/download-ng.html>
2. Download a version of TomEE that is compatible with your AppWorks Platform version.
3. Unzip to C:\Program Files\
4. Rename the TomEE version to TomEE.

Creating a TomEE user

To create a user named TomEE:

1. From the Start menu, select **Run**.
2. Type **lusrmgr.msc** and click **OK**.
The Local Users and Groups window opens.
3. Right-click **Users** and select **New User**.
The New User window opens.
4. For:

User name	Type a user name of your choice. For example: TomEE.
Password Confirm password	Type a password of your choice. For example: 123#TomEE.
User must change password at next logon	Clear the check box.
User cannot change password	Select this check box.
Password never expires	Select this check box.
Account is disabled	Leave this check box unselected.

5. Click **Create**.
The User is created.
6. Write the user ID and password details on the Installation Worksheet.
7. Click **Close**.
8. On the Local Users and Groups window, select **Users** to view the newly created User (TomEE).
The Local Users and Groups window opens.
9. Right-click the **TomEE** user and select **Properties > Member Of**.
10. Select **Users** and click **Remove**.
The list must now be empty.
11. Click **OK** to save changes and exit the TomEE Properties.
12. Close the Local Users and Groups window, and then continue with [Granting TomEE access to the installation directory on page 31](#).

Granting TomEE access to the installation directory

To grant the TomEE user access to the installation directory:

1. Navigate to `C:\Program Files`
2. Right-click the **TomEE** folder and select **Properties > Security > Edit**.
The Permissions for TomEE dialog box opens.
3. Click **Add**.
The Select Users or Groups dialog box opens.
4. For:

Object Types	In the Object Type dialog box, clear all object types except for Users, and then click OK .
Locations	In the Locations dialog box, select your local server name, and then OK .
Check Names	In the Object names to select section, type TomEE , and then click Check Names to verify the user name.

- Click **OK**.
The Permissions for TomEE dialog box returns with TomEE already selected in the Group or user names box.
- Under **Group or user names**, select **TomEE** and then for **Permissions for TomEE**, grant **Full control**, and click **OK**.
- Click **OK** to exit the TomEE Properties dialog box.

Adding a default value environment variable

To add an environment variable that provides default values to the AppWorks installer:

- From the Start menu, select **Run**.
- Type **sysdm.cpl**, and then click **OK**.
The System Properties dialog box opens.
- Click **Advanced > Environment Variables**.
The Environment Variables dialog box opens.
- Under System variables:
 - Scroll to see whether an existing `CATALINA_HOME` variable is available. If one exists, select the `CATALINA_HOME` variable, and then click **Edit**.
 - If the `CATALINA_HOME` variable does not exist, click **New**.

The Edit or New System Variable dialog box opens.

- For:

Variable name	Type: <code>CATALINA_HOME</code>
Variable value	Set the value to: <code>C:\Program Files\TomEE</code>

6. Click **OK** to save the variable.
7. Click **OK** to exit the Environment Variables dialog box.
8. Click **OK** to close the System Properties dialog box.

Installing the TomEE service

To install TomEE service:

1. Open a command prompt with Administrator privileges in `C:\Program Files\TomEE\bin`.
2. To install the Apache TomEE service, type `service.bat install`, and then press **Enter**. A message indicating TomEE has been installed appears on the command prompt.
3. Close the command prompt.
4. From the Start menu, select **Run**.
5. Type **services.msc** and then click **OK**.
6. Right-click **Apache TomEE** and click **Properties > Log On**.
The Log On tab displays.
7. For:

This account	Click Browse to select the TomEE user. The Select User dialog box opens.
Object Types	Click this option to select Users . Clear all object types except for Users, and then click OK . Note: The TomEE user must be in the following format: <domain name>\<user name>. AppWorks does NOT support the following users: <ul style="list-style-type: none"> ■ Local System ■ User names in the User Principal Name (UPN) format. For example: <user name>@<domain name> is not supported.
Locations	Click this option to select your local server.
Object names to select	Type TomEE , click Check Names to verify the user name, and then click OK .
Password	Type the password specified while creating the TomEE user, and then click OK . See the Installation worksheet on page 17 for the user and password details. A dialog box opens indicating the account <code>.\TomEE</code> has been granted the Log On As A Service right.

8. Close the Service Manager window.

Updating the TomEE configuration

To update the TomEE configuration:

1. Navigate to the `<TomEE_installdir>\bin` and double-click **TomEE.exe**. The Apache TomEE Properties Window opens.
2. Click the **Java** tab.
4. Under **Java Options**, add the following text:

```
-Dcom.sun.management.jmxremote.port=9090
-Dcom.sun.management.jmxremote.ssl=false
-Dcom.sun.management.jmxremote.authenticate=false
-Dbus.xml.vm.maxsize=2048
```

To change the memory settings:

5. Change the **Initial memory pool** to 1024.
6. Change the **Maximum memory pool** to 2048.
7. Click **OK**.

Configuring JDBC driver for TomEE

Use one of these procedures based on your database to configure the JDBC driver for TomEE. It ensures that the JDBC driver can be used with all the AppWorks components.

Configuring for MS SQL

To configure JDBC driver for TomEE on MS SQL:

1. From the link [https://msdn.microsoft.com/en-us/library/mt683464\(v=sql.110\).aspx](https://msdn.microsoft.com/en-us/library/mt683464(v=sql.110).aspx), download the Microsoft JDBC Driver 7.2 for SQL Server.
2. After the file is downloaded, extract the Microsoft JDBC driver.
3. Copy the `mssql-jdbc-7.2.1.jre11.jar` file to the `<TomEE_installdir>\lib` folder. For example: `C:\Program Files\TomEE\lib`

Note: Ensure that the lib folder contains **only** the supported version of the JDBC driver.

4. Add the `<TomEE_installdir>\lib\mssql-jdbc-7.2.1.jre11.jar` file to the system CLASSPATH variable.

Note: Ensure that the CLASSPATH contains **only** the supported version of the JDBC driver.

5. **Optional:** If MS SQL Server is used in Windows Authentication mode:
 - Copy the 64-bit `sqljdbc_auth.dll`, shipped with the MS SQL server JDBC driver to the `<TomEE_installdir>\bin` folder.
 - Navigate to the `<TomEE_installdir>\bin` and double-click `TomEE.exe`.
 - The Apache TomEE Properties window opens.
 - Navigate to the Java tab > Java options. Ensure that the `-Djava.library.path` contains the AppWorks Platform's lib, in addition to the `jdbc_auth.dll`'s path.
 Example: `Djava.library.path=C:\Program Files\sqljdbc_4.0\enu\auth\x64;C:\Program Files\OpenText\AppWorksPlatform\defaultInst\lib`
 - Add the `<TomEE_installdir>\bin` folder to the system PATH variable.
 - Ensure that the user under which TomEE/AppWorks Platform runs is authorized in MS SQL Server. For details, see Using Windows Authentication to access SQL Server topic in the product documentation.
6. **Optional:** Enable XA transaction settings as follows:
 - Copy the 64-bit `sqljdbc_xa.dll` from the `<JDBC_driver_installdir>\xa\x64` to the `<MS SQL Server_installdir>\Binn` folder of every MS SQL Server computer.
 - Execute the database script `xa_install.sql` available in the `<JDBC_driver_installdir>\xa` folder. You need administrative privileges on SQL Server to execute/register a DLL.
 - [Enable XA Transaction](#) for MSDTC on the MS SQL Server computer and restart the MS SQL Server.

Configuring for Oracle

The Oracle OCI driver support is deprecated. However, OpenText recommends using Oracle thin driver for database connectivity.

To configure JDBC driver for TomEE on Oracle:

1. From the link <https://www.oracle.com/technetwork/database/application-development/jdbc/downloads/jdbc-ucp-183-5013470.html>, select **Accept License Agreement** to download the version 18.3 `ojdbc8.jar` file.
2. Copy the JAR to the `<TomEE_installdir>\lib` folder.
 For example: `C:\Program Files\TomEE\lib`
Note: Ensure that the lib folder contains **only** the supported version of the JDBC driver.
3. Add the `<TomEE_installdir>\lib\ojdbc8.jar` file to the system CLASSPATH variable.
Note: Ensure that the CLASSPATH contains **only** the supported version of the JDBC driver.

4. **Optional:** If Oracle is installed on a Linux computer, do the following:
 - a. Open `$JAVA_HOME/jre/lib/security/java.security` file.
 - b. Modify the `securerandom.source` property value to `file:/dev/./urandom`
5. **Optional:** Enable XA settings as follows:
 - a. Start Oracle SQL command prompt.
 - b. Connect with the credentials: `sys as sysdba`.
 - c. Grant the following rights:
 - Grant `select` on `sys.dba_pending_transactions` to `<user name>`;
 - Grant `select` on `sys.pending_trans$` to `<user name>`;
 - Grant `select` on `sys.dba_2pc_pending` to `<user name>`;
 - Grant `execute` on `sys.dbms_system` to `<user name>`;

Note: `<user name>` refers to the credentials of the AppWorks user who connected to the database (as specified in the AppWorks Database configuration).

Configuring for PostgreSQL

To configure JDBC driver for TomEE on PostgreSQL:

1. From the following link, <https://jdbc.postgresql.org/download.html>, download the relevant JDBC driver. For example: `postgresql-42.2.5.jar`
2. Copy the jdbc driver jar (for example, `postgresql-42.2.5.jar`) to the `<TomEE_installdir>\lib` folder.
For example: `C:\Program Files\TomEE\lib`

Note: Ensure that the lib folder contains **only** the supported version of the JDBC driver.

3. Add the `<TomEE_installdir>\lib\postgresql-42.2.5.jar` file to the system CLASSPATH variable.

Note: Ensure that the CLASSPATH contains **only** the supported version of the JDBC driver.

4. **Optional:** Enable XA transaction settings by specifying the `max_prepared_transactions` parameter in the `<PostgreSQL_installdir>\postgresql.conf` file. The value must be at least as large as the "max_connections" value.

Configuring TomEE ports

To modify the TomEE port:

1. Navigate to `<TomEE_installdir>\conf`.
2. Right-click `server.xml` and select **Edit**.
The `server.xml` file opens.

3. Edit the following items:

- Change the Server shutdown port from 8005 to 8006.
- Change the Connector port from 8080 to 81 (recommended).
- Append to Connector port, add the attribute `URIEncoding="UTF-8"`
- Change the AJP 1.3 Connector port from 8009 to 8010.

Note: Port 8080 is typically reserved for Tomcat OTDS installation and port 80 for other programs that use IIS during installation.

After edits, the sample Connector configuration is as follows:

```
-->
<Connector port="81" protocol="HTTP/1.1"
    connectionTimeout="20000"
    redirectPort="8443"
    xpoweredBy="false"
    server="Apache TomEE"
    URIEncoding="UTF-8" />
<!-- A "Connector" using the shared thread pool-->
```

4. Save and close the file.

Important: If running a monolithic system, verify ports and ensure that Tomcat, TomEE, and IIS are running on different ports. If you change the default port number of the Connector port to any other port number, you must change the `redirectPort`, `serverPort`, and the Connector port of AJP to other ports that do not conflict with the Tomcat ports. Write the port you use on the Installation Worksheet.

To update the AppWorks Platform configuration:

After changing the port number in TomEE, you must update the AppWorks configuration. The property `com.cordys.node.url` must point to the localhost URL including protocol and port number. It must be updated when SSL is enabled on the Web server or when the port number is changed.

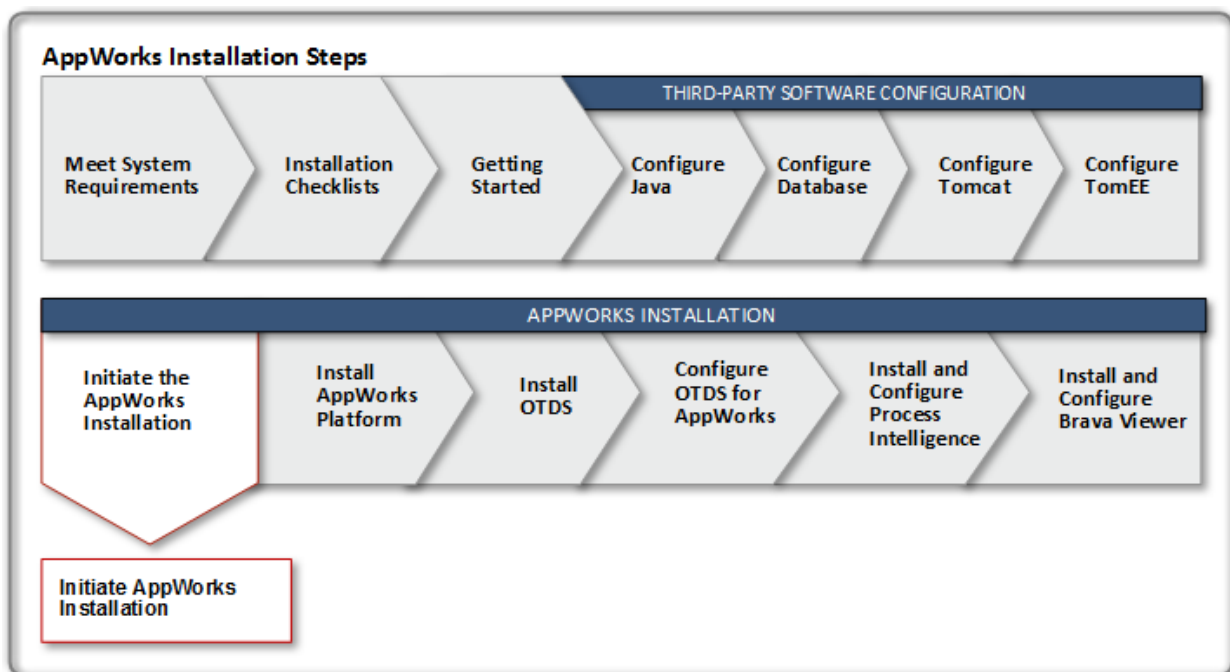
1. Navigate to `<AppWorks Platform_installdir>/config` folder, open `wcp.properties`, and then enter the following:

Property	Value
<code>com.cordys.node.url</code>	<p><code>http://localhost:<port number></code></p> <p>If a non-default port number is used, you must include it in the URL.</p> <p>For example: <code>http://localhost:81</code></p> <p>Note: See Using HTTPS in AppWorks Configuration guide on My Support for configuring TomEE with HTTPS.</p>

Chapter 6

Initiating AppWorks installation

The next step for installing AppWorks is to initiate the AppWorks installation bundle.



The AppWorks installer can initiate multiple installations in sequence. The procedures in this document instruct you to initiate the installer independently for each component, as there are manual configurations that must be completed before you initiate installation for the next component. Initiating independent installations ensures that the install wizards do not start another installation prematurely.

The installer initiates the following component installations:

- OpenText AppWorks Platform
- OpenText Directory Services
- OpenText Process Intelligence
- OpenText Brava

Prerequisite: Before initiating the AppWorks installation:

- Create a database user for the database installation.
- Install the JDBC driver and added the relevant JDBC jar for your database to the following:
 - the CLASSPATH
 - the <TomEE_installdir>\lib folder

See [Configuring JDBC driver for TomEE on page 34](#) for more details.

Important: Do not create a database user containing a period (.) in the user name.

To initiate AppWorks installation:

1. Navigate to the <extracted_installdir> and extract the contents of the zip file installation bundle that you copied to this folder.
The contents of the zip file are listed.

The following table describes the contents of this folder:

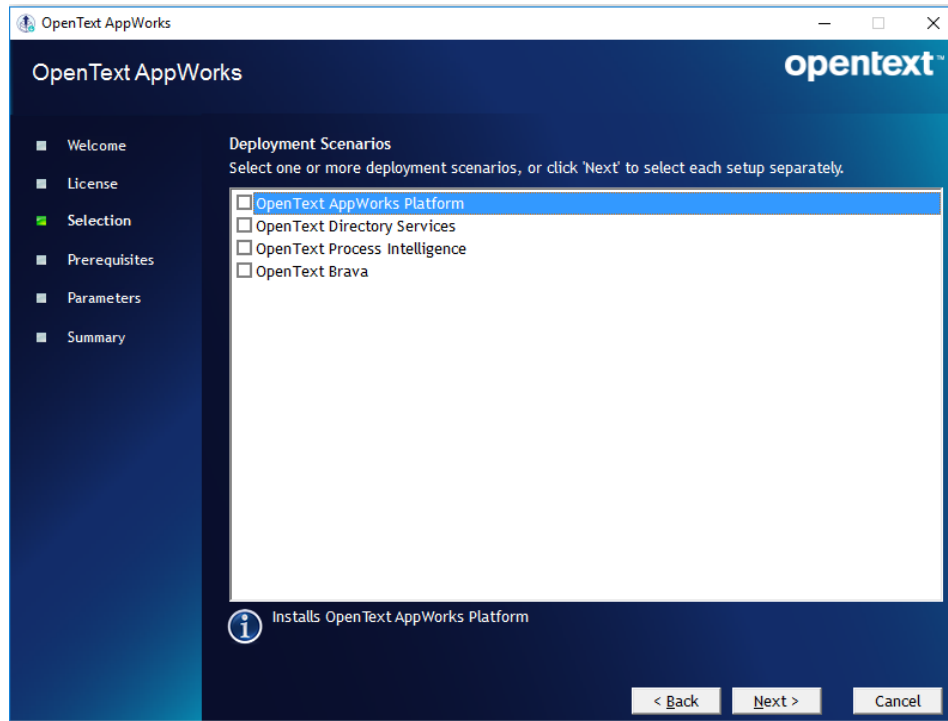
Item	Description
OpenTextBrava	Contains the OpenText Brava Enterprise installer.
OpenTextCordysRESTClient	Contains the JAR files that are used to invoke the REST APIs for AppWorks Platform.
OpenTextDirectoryServices	Contains the OpenText Directory Services installer and AppWorks Platform Connector for pushing users and roles from OTDS to AppWorks Platform.
OpenTextProcessIntelligence	Contains the OpenText Process Intelligence installer.
OpenTextAppWorksPlatform	Contains the OpenText CARS and OpenText AppWorks Platform (AppWorks Platform) installer files. Additionally, it also contains the certificates, application packages that are used for installation, command line installation scripts, release notes, installation and configuration guides, and so on.
Mastersetup.exe	Master installer to install all components of AppWorks.
mastersetup.xml	Input file for AppWorks installer.

2. Navigate to the <extracted_installdir> and right-click **Mastersetup.exe** and **Run as Administrator**.
The OpenText AppWorks Installer dialog box opens.
3. Click **Next**.
The License Agreement dialog box opens.
4. Review the license agreement carefully by scrolling to the bottom of the agreement.
Check the **I accept the terms in the License Agreement** check box, and click

Agree.

The Deployment Scenarios dialog box opens.

Important: You can select or clear the options of the components to be installed based on your business requirements. This guide provides instructions based on installing each component separately. See the installation and configuration instructions provided in the relevant sections for more information.



5. Check the **OpenText AppWorks Platform** check box and click **Next**.

Note: You can select AppWorks Platform and OpenText Directory Services; however, OpenText recommends that you do NOT select other products because it is optional. The installation process reflects separate instructions for each option.

The Product Groups dialog box opens with Product Groups and Components collapsed.

6. Expand **OpenText AppWorks Platform** and verify the following are selected:
 - OpenText AppWorks Platform
 - OpenText CARS 2.6
 - OpenText AppWorks Platform 16.7

Note: If other components are selected, clear these options. The installation for these components is called independently.

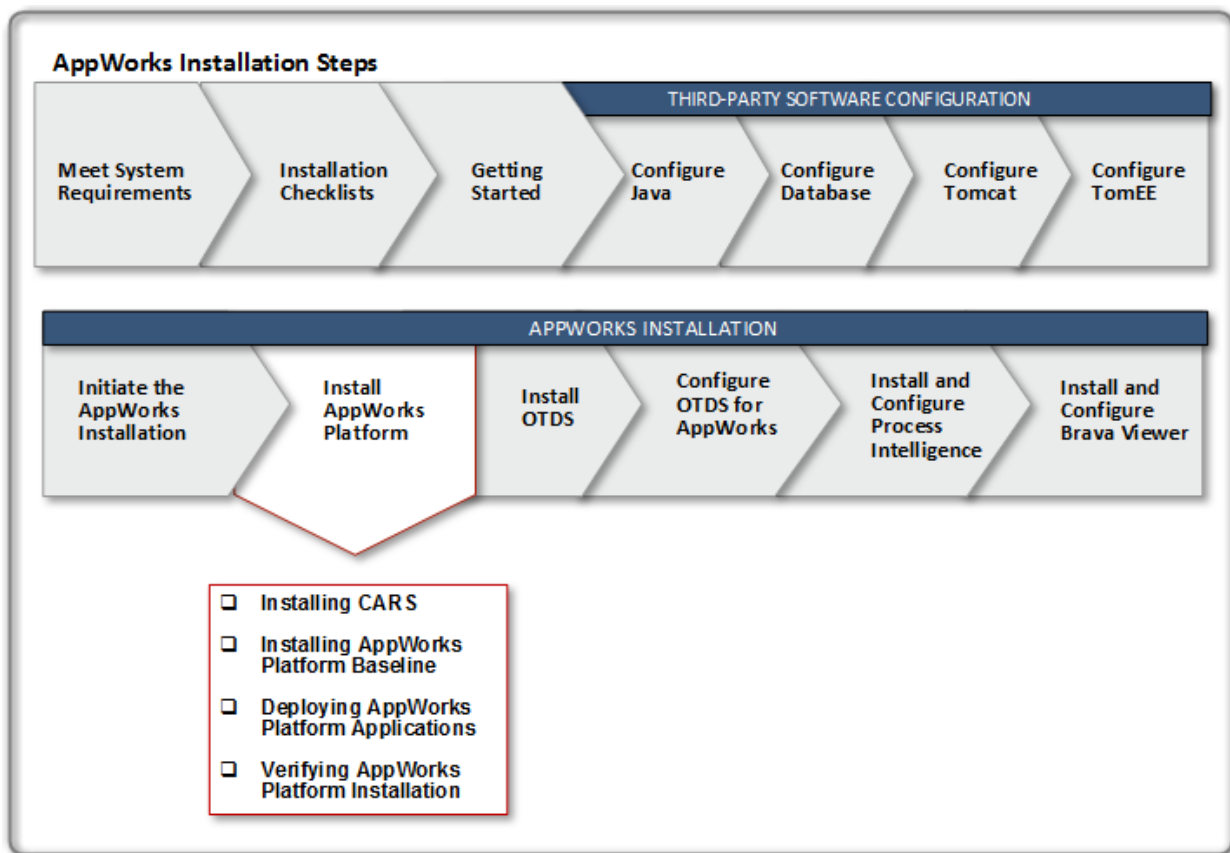
7. Click **Next**.
The Summary dialog box opens showing the components you selected.

7. Verify that all components from the previous step are shown and click **Install**.
The InstallAnywhere wizard is initiated.
When initiation is complete, the CARS Welcome dialog box opens.
8. Continue with [Installing CARS on page 44](#).

Chapter 7

Installing AppWorks Platform

The next step for installing AppWorks is to install AppWorks Platform. The AppWorks Platform installation comprises three stages: CARS, baseline, and applications.



AppWorks Platform installation considerations

AppWorks Platform, when installed as part of the AppWorks bundled installation, can be installed on the same computer as the other AppWorks components or on a different computer. Additionally, multiple instances of AppWorks Platform can be installed on the same computer. Each instance is identified with a unique name and is independent of other instances.

Possible installation scenarios include:

- Host multiple instances of AppWorks Platform on a single computer pointing to a single CARS.
- Host multiple instances of AppWorks Platform on a single computer pointing to different instances of CARS.
- Host AppWorks Platform along with earlier versions on a single computer.

Note: Although AppWorks Platform supports using a single CARS instance for multiple AppWorks Platform instances, it is strongly recommended that you use one CARS instance per AppWorks Platform instance. This is useful in backup and restore scenarios, where you need to stop CARS to restore LDAP content of a AppWorks Platform instance. This results in other AppWorks Platform instances being stopped as well. Therefore, having a dedicated CARS instance for each AppWorks Platform instance helps avoid such situations.

Two or more installations of AppWorks Platform can share the same directory service (CARS) and distribute the load of service requests between themselves. This setup is preferred in high availability required environments. To configure AppWorks Platform in high availability mode to manage failover, see the AppWorks Platform High Availability Deployment Guide available on [My Support](#).

This topic includes the following:

- [Installing CARS on page 44](#)
- [Installing AppWorks Platform baseline on page 46](#)
- [Deploying AppWorks Platform applications on page 51](#)
- [Verifying AppWorks Platform installation on page 54](#)

Installing CARS

AppWorks Platform requires a repository where it can store all its information about organizations, users, service containers, services, and other objects. CARS is a Lightweight Directory Access Protocol (LDAP) service provided and supported by AppWorks Platform.

The AppWorks Installation wizard installs CARS. It can be installed on the same computer where AppWorks is installed or on a different computer.

To install CARS:

1. On the CARS Welcome dialog box, click **Next**.
The Third-Party Software License Agreements dialog box opens.
2. Review the license agreement, select the **I accept the terms of the License Agreement** option and click **Next**.
The Instance Name dialog box opens.
3. Accept the default instance name `defaultinst` or type an Instance Name for this instance and click **Next**.

Note: This can be a name of your choice. Write this name on the Installation Worksheet for future reference.

The Installation Folder opens.

4. Accept the default folder location and click **Next**.

Note: If installing CARS on a separate computer, type the absolute path to where the service is created.

The Server Configuration dialog box opens.

5. Do the following:

Network enabled installation	Select the option. Note: OpenText recommends that you do NOT change to a Standalone installation. However, if you change it, you can enter your own user information on the next dialog box.
Server Identifier	Type the Fully Qualified Domain Name (FQDN) location for the CARS installation if different from the default.
Server Port	Accept the default port value.
Suffix	Accept the default suffix value.

6. Write the port number on the Installation Worksheet.

Note: This might be required if you are installing AppWorks Platform in a Primary-Distributed environment.

7. Click **Next**.

The User Credentials dialog box opens.

8. Accept the default user name or provide a desired user name.

Where: cn=<username>, o=<domainSuffix>

For example: cn=Directory Manager, o=mycompany.com

9. Type a value for **Password** and **Confirm Password**.
10. Write the **User Name** and **Password** on the Installation Worksheet.
11. Click **Next**.

The Pre-installation Summary dialog box opens.

12. Review the details in the dialog box and click **Install**.
The installation begins and on successful completion, the Installation status dialog box opens.

13. Click **Done**.
The CARS installation is complete. The installation preparation continues. When preparation is complete, the Welcome dialog box opens.
14. Continue with Installing AppWorks Platform baseline.

Installing AppWorks Platform baseline

After installing CARS, the next step in the AppWorks Platform installation is to install the AppWorks Platform baseline.

Note: See the Installation Worksheet for field parameter values.

To install AppWorks Platform:

1. On the AppWorks Platform Welcome dialog box, click **Next**.
The License Agreement dialog box opens.
2. Review the license agreement for AppWorks Platform by scrolling to the bottom of the agreement, select **I accept the terms of the License Agreement**, and click **Next**.
The Third-party Software License Agreements dialog box opens.
3. Review the license agreement for third-party software by scrolling to the bottom of the agreement. Select **I accept the terms of the License Agreement**, and click **Next**.
The CARS Information dialog box opens.
4. For:

CARS installed on this computer	Select this option.
CARS installed on a different computer	Select this option only if you are using multiple computers and have installed CARS on a different computer.
CARS is running under secure mode	Automatically selected.
CARS Host	Automatically populated.
Port Number	Automatically populated.
Suffix	Automatically populated.
CARS Certificate Path	Automatically populated.
User Name	Automatically populated.
Password	Type the CARS password. See the Installation Worksheet for details.

5. Click **Next**.
The Advanced Configurations dialog box opens.

6. For:

Installation mode	<ul style="list-style-type: none"> ■ Network enabled installation - Select this option. ■ Standalone installation -
Install application packages	Automatically selected.
Minimize memory footprint	Clear this check box.
Enable caching of web content	Automatically selected.
Maximum age	Default age is 15 Minutes.

7. Click **Next**.

The Instance Information dialog box opens.

8. Accept the default value or type a name for this instance, and then click **Next**.

The License Information dialog box opens.

9. For:

License Mode	Select Single .
Registered Customer Name	Type the name of the customer associated with this product.
Registered Site Name	Type the site name provided with the purchase of the product. Refer to the Installation Worksheet or your sales materials.

10. Click **Next**.

The License Key Information dialog box opens.

11. For the License Key information, do one of the following:

- Leave the check box selected if you know the password for the site, and then type the password provided by OpenText in **Password for the site (<site name>)**.
- Clear this check box if you have the license key, and then type the key provided by OpenText in **License Key**.

Tip: Refer to the Installation Worksheet or your sales materials for the relevant details

12. Click **Next**.

The Installation Folder dialog box opens.

13. Click **Next**.

The TomEE Details dialog box opens.

14. Accept the default values for the following values.

CATALINA HOME	Automatically populated.
CATALINA BASE	Automatically populated.
Tomcat Service	Automatically populated.
Tomcat Connector	Automatically populated.
Tomcat OS service name	Type the Tomcat OS service name. Note: The default value of Tomcat OS service name is TomEE . However, if you have already installed TomEE with another service name, you must enter that name here.

15. Click **Next**.
The Administrator Settings dialog box opens.
16. Type and confirm the password for the administrator user.
17. Write the administrator password on the Installation Worksheet.
18. Click **Next**.
The Database Information dialog box opens.
19. Enter the required values as specified below. The fields vary based on the Database Type selected.

■ **For MS SQL server:**

Database Type	Select MS SQL Server from the Database Type list.
Server name	Type the full computer name of the database where the installation is taking place. (From the Desktop, right-click and select Properties. Obtain the Computer name.) Optionally, you can also type the SQL instance name along with the server name as <computername>/[instancename]. For example: AppWorks.opentext.net/SQL2012. Note: The database might not be the local computer where you are installing AppWorks Platform.
Port	Accept the default of 1433.
Authentication type	Accept the default of SQL Authentication.
User Name and Password	Type a new name and password for this AppWorks Platform installation. If SQL Server database is used with Windows Authentication as the Authentication type, the database user details are hidden. The user name and password details given in the Monitor Service User panel shall be used to connect to

	the database.
Database Name	Type a unique database name.
Use SSL for connectivity	Leave check box cleared. Note: If you want to use secured connectivity using SSL, ensure that the database server is configured to use SSL, and then select this check box.
Create New Database	Select this check box. When selected the DBA User name and Password fields are displayed.
Use same DB for Logger	Select this check box.
DBA User Name and DBA Password	Type a user name and password for the database administrator.

■ **For Oracle:**

Database Type	Select Oracle from the Database Type list.
User Name and Password	Type a new name and password for this AppWorks Platform installation.
Database Service Name	Type the unique database name of the service, which is used to connect to this database, entered during installation or database creation.
Use thin client	Select this check box. When checked, the Server name and Port fields are enabled.
Server name	Type the full computer name of the database where the installation is taking place. For example: <code>sales.acme.com</code>
Port	Accept the default of 1521.
Create New User	Select this check box. When checked the DBA User name and Password fields are displayed.
Use same DB for Logger	Select this check box.
DBA User Name and DBA Password	Type a user name that has SYSDBA privilege in the format, <code><user name> as sysdba</code> , and password for this user.

■ **For PostgreSQL**

Database Type	Select PostgreSQL from the Database Type list.
Server name	Type the fully qualified name of the database server. For example: <code>sales.acme.com</code>

Port	Type the port number of database server. Default is 5432
User Name and Password	Type an existing PostgreSQL user name and password.
Database Name	Type a unique database name for new database.
Use SSL for connectivity	Leave check box cleared.
Create New Database	Select this check box. When checked, the DBA User Name and Password fields are displayed. Note: AppWorks Platform creates all database objects in the default schema. For example, by default, public is the default schema in PostgreSQL and all database objects will be created in this schema.
Use SSL for connectivity	Leave check box cleared. Note: If you want to use secured connectivity using SSL, ensure that the database server is configured to use SSL, and then select this check box.
Use same DB for Logger	Select this check box.
DBA User Name and DBA Password	Type PostgreSQL user name and password for the database administrator.

19. Click **Next**.
The Monitor Service User Details dialog box opens.
20. The TomEE service logon user name is populated automatically. Type the appropriate password and click **Next**.
The Please Wait dialog box opens advising to wait while AppWorks Platform is configured.
The Database Settings dialog box opens.
21. Click **Next**. The PostgreSQL DB Tablespace Info page appears.
Optional: This page appears only if you selected PostgreSQL as the database in the Database Information page. Do one of the following:
 - To create a new tablespace, select **Create new tablespace** and type a name and path where the tablespace will be located in the database.
 - To use an existing tablespace, select **Use existing tablespace** option and type the name of the tablespace.
22. Click **Next**.
The Please Wait page appears advising to wait while the AppWorks Platform is configured.
A Database Settings dialog box opens displaying the recommended database configuration. Read the recommendation and click **OK**.
The JMX Settings page appears.

23. Click **OK** to continue.
The JMX Settings dialog box opens.
24. Enter the **User Name** and **Password** to define the user details for the JMX console and click **Next**.
The Please Wait dialog box opens advising to wait while AppWorks Platform is configured.
When the process is complete, the Pre-installation Summary dialog box opens.
25. Review the installation summary list and click **Install**.
The installation procedure continues automatically. A series of progress screens appear including a TomEE script execution bar.

On successful completion, a dialog box opens.
26. Click **Done**.
The Please Wait dialog box opens.
A browser window opens to the AppWorks Platform Explorer and begins deploying mandatory applications. Numerous applications are deployed and can take several minutes.
27. Proceed with deploying applications as explained in [Deploying AppWorks Platform applications on page 51](#).

Note: If a Welcome to the OpenText Directory Services install wizard opens, leave this open in the background while you continue with Deploying AppWorks Platform Applications.

Deploying AppWorks Platform applications

Note: See the Installation Worksheet for the field parameter values.

If you selected AppWorks Platform authentication during the baseline installation, you must provide the same user name and password to proceed and load the application packages.

To deploy AppWorks Platform applications:

1. From the AppWorks Platform Explorer that launched at the conclusion of the prior section, the Deploying mandatory application is displayed.

The Enter User Credentials dialog box opens.
2. Type the AppWorks Platform Administrator User Name and Password and click **Sign In**.
Refer to the Installation Worksheet for the user details.
The installer prepares to deploy product applications.

After deploying a number of applications, the database connection is deployed.
During this deployment, the screen updates displaying a Loading message.
The User Inputs window opens to the CWS Core options.

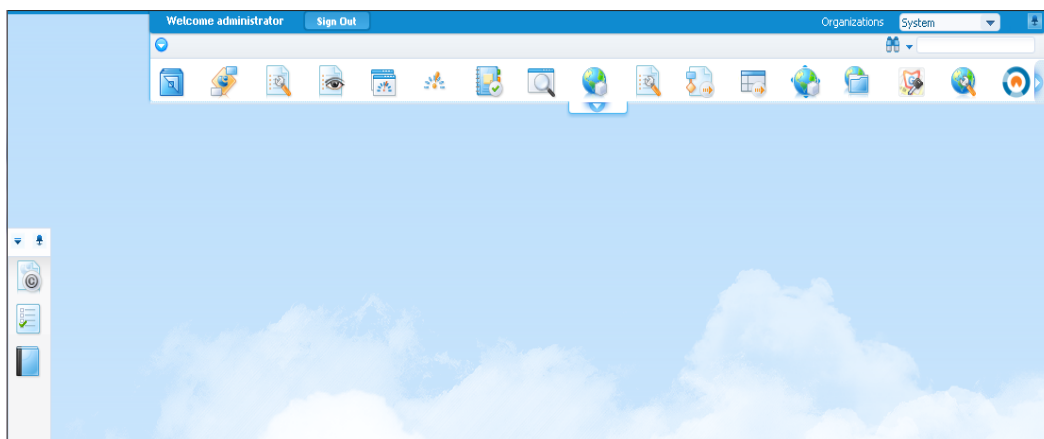
3. Do one of the following:

- Select **Use same inputs for all applications** if you want to use the same database configuration details for all the applications listed under Select Package To Configure Details.
- Select **Configure different inputs for Applications** if you want to provide different database configuration details for different applications listed under Select Package To Configure Details.
Ensure that the following special considerations are met when you select this option.

For applications	Do the following
Cordys CWS Core	Select Cordys System as the database configuration.
Cordys Business Activity Monitoring	Select the same database configuration for Cordys Business Process Engine and Cordys Notification applications.
OpenText Entity Runtime	Select the same database configuration for Cordys Business Process Engine, Cordys Notification, OpenText Entity Runtime, and OpenText Document Store Services applications.
Cordys MDM	For a production environment, select a different database configuration from the database configuration selected for Cordys Business Activity Monitoring. In this event, specify the options for the new database configuration.

4. For **Select Database Configuration**, select the relevant database configuration.
All other fields are automatically populated.
 5. Click **Next**.
A summary page appears with the details of each application.
 6. **Optional**: Check the **Revert on Failure** check box.
 - If checked and the deployment fails, the application package that failed is reverted to its previous state. The subsequent deployment attempt proceeds from the failed application package. Default 15 minutes – timeout in minutes
 - If unchecked and an application fails to load, the application moves into an Incomplete state and the subsequent attempt of installation resumes from the point of failure.
 7. Click **Deploy**.
The deployment of the application packages starts.
Deployment can take more than 30 minutes to complete.
- Note:** If any issues arise during the deployment of the CAP files, increase the JVM size. Go to **System Resource Manager > Cap service container** and increase the JVM size to **512** in the JRE configuration tab.
- After deploying all the applications, a summary page displays a list of all deployed application packages.
8. Click **Finish**.
Deployment of the application packages is complete and the AppWorks Platform installation is complete.
The AppWorks Platform sign in page opens.
 9. Enter the AppWorks Platform **User Name** and **Password** and click **OK**.
The AppWorks Platform Explorer opens.

The default screen is displayed.



10. Continue with [Verifying AppWorks Platform installation on page 54](#).

Verifying AppWorks Platform installation

Verify that AppWorks Platform is configured properly and the database tables are initiated.

To verify the application link:

1. Open Internet Explorer and type:
`https://<server>:<port>/home/<organization>/app/start`

Where:

<server>	is the server where AppWorks Platform is installed
<port>	is the port number associated with the installation
<organization>	is the organization where the installation is installed


For example: `http://localhost:81/home/system/app/start`

The Enter User Credentials dialog box opens.

2. Type the **User name** and **Password** and click **Sign In**.
The default layouts page displays.

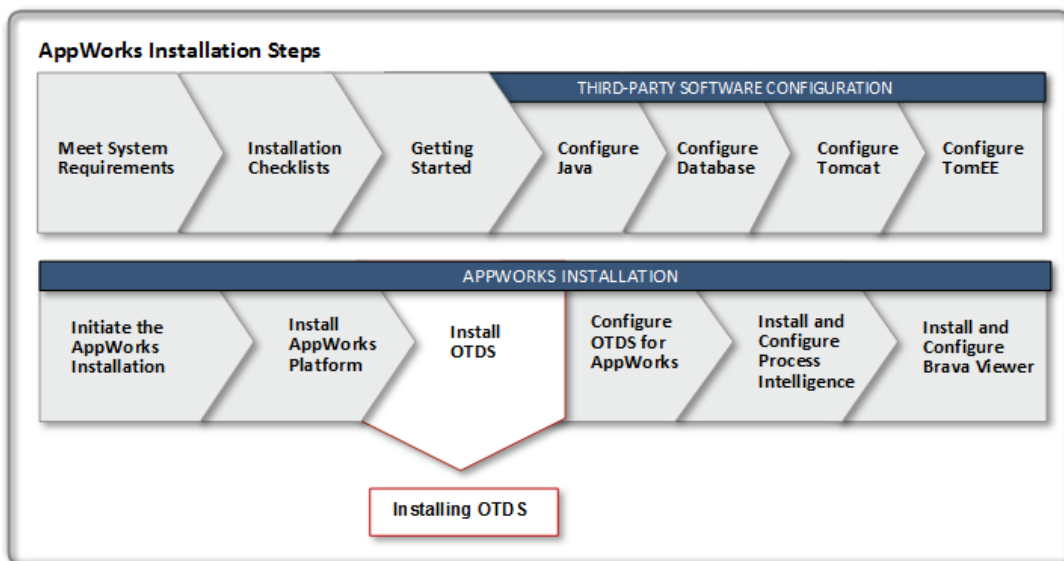
Tip: When you test the application, if the browser freezes with a screen that displays `Loading application`, you must close the browser and test again.

Hardening AppWorks Platform security

After the installation of AppWorks Platform, ensure to secure the environment. For information on securing AppWorks Platform and related components including OTDS, see the Hardening the Security of AppWorks Platform topic in the help () accessible from the shortcut bar on the AppWorks Platform interface.

Chapter 8

Installing OpenText Directory Services



Before you begin:

- OpenText recommends that the user installing or upgrading OTDS has administrative privileges.
- Ensure that the <TomEE user> has Read and Write access on the OTDS installation directory.

Installing OpenText Directory Services

To install OTDS:

1. Navigate to the <extracted_installdir> and right-click **Mastersetup.exe** and **Run as Administrator**.
The AppWorks Installer dialog box opens.

2. Click **Next**.
The License Agreement dialog box opens.
3. Review the license agreement carefully by scrolling to the bottom of the agreement. Check the **I accept the terms in the License Agreement** check box, and click **Agree**.
The Deployment Scenarios dialog box opens.
Important: You can select or clear the options of the components to be installed based on your business requirements. This guide provides instructions based on installing each component separately. Refer to the installation and configuration instructions provided in the relevant sections for more information.
4. Select the **OpenText Directory Services** check box and click **Next**.
5. Expand **OpenText Directory Services** and verify if OpenText Directory Services 16.0.2 is selected.
6. Click **Next**.
The Summary dialog box opens showing the components you selected.
7. Verify that all components from the previous step are shown and click **Install**.
The InstallAnywhere wizard is initiated.
8. When initiation is complete, the OpenText Directory Services Welcome page appears.
9. Click **Next**.
The License Agreement dialog box opens.
10. Review the license information by scrolling to the bottom of the text. Check the **I accept the terms in the License Agreement** check box and click **Next**.
The Destination Folder dialog box opens.
11. Accept the default location and click **Next**.
The Application Server dialog box opens.
12. Leave the default, **Apache Tomcat**, and click **Next**.
The Installation Type dialog box opens.
13. Leave the **Please check this box if you wish to setup the server as a replication server** check box unchecked and click **Next**.
The Java Virtual Machine dialog box opens.
14. Click **Next**.
The Apache Tomcat Directory dialog box opens.
15. Accept the default value and click **Next**.
The Directory Services Parameters dialog box opens.

16. Accept the default port numbers and click **Next**.

Note: Make sure that no other programs are using the default directory services ports. If another program is using these ports, the installer does not allow you to proceed.

The OTDS Administrator dialog box opens.

17. For:

Enforce a complex password for otadmin@otds.admin	Uncheck this check box.
Password Confirm Password	Type the OTDS Administrator user name and password.

18. Write the password in the Installation Worksheet.

19. Click **Next**.

The Data Import dialog box opens.

20. Do one of the following:

- If this is a new installation, accept the default (No import) option and click **Next**.
- If data exists, select **Import Data from OpenText Directory Services <version>**, type the relevant path, and then click **Next**.

See the OTDS Administrator's Guide for details on importing data from the applicable version.

The Ready to Install dialog box opens.

21. Click **Install** to initiate the OTDS installation.

The Installing the product dialog box opens displaying a progress bar.

Note: Depending on the server configuration, the installation can take more than 5 minutes.

The Completing the OpenText Directory Services <version> installation dialog box opens.

22. Click **Finish**.


The OTDS installation completes.

Verifying the OTDS installation

To verify OTDS installation:

1. Access a browser and type the following URL:
`http://<server name>/otds-admin`
The OTDS sign in dialog displays.
2. Enter the relevant credentials and click **Sign in**.
The OTDS web administration page appears.

This concludes the OpenText Directory Services installation process.

Note: After installing and verifying OTDS, you can configure OTDS as the authentication mechanism for AppWorks Platform. See the Configuring OTDS for AppWorks Platform topic in the help () accessible from the shortcut bar on the AppWorks Platform interface for more details.

Chapter 9

Configuring OpenText Directory Services

This section identifies the configuration of OTDS required to support AppWorks.

Topics include:

- [Configuring OTDS for AppWorks Platform on page 59](#)
- [Configuring AppWorks Platform for OTDS authentication on page 61](#)
- [Configuring OTDS authentication for an organization on page 67](#)
- [Disabling the authentication handler on page 76](#)

Configuring OTDS for AppWorks Platform

Configuring OTDS for AppWorks Platform consists of the following tasks:

- Adding an OTDS partition
- Adding an OTDS user

Adding an OTDS partition

To add a AppWorks Platform OTDS partition:

1. Launch a browser and type the following URL:
`http://<hostname>:<tomcat port no>/otds-admin` and sign in with the appropriate credentials.
For example:
`http://localhost:8080/otds-admin`
Note: Retrieve this user name and password from the Installation Worksheet or contact your system administrator.
The OTDS Administration page appears.
2. Click **Partitions**.
The Partitions dialog box opens displaying the `otds.admin` partition.

Note: The `otds.admin` partition was created during the installation.

3. Click **Add > New Non-synchronized User Partition**.
4. Enter a name and description (these can be anything). The description is optional.
AppWorks Platform Partition is the recommended name, but it is not required. The remainder of this document assumes the partition has this name.
5. Click **Save**. The new partition is added.
6. **Optional, but recommended.** For the new partition just created, click **Actions > Password Policy**.
7. Clear the **Use global policy** check box, and set the **Password Quality** and **Security Options** to the required setting for your environment.
8. Click **OK**.
The Partitions dialog box displays the newly created partition.
9. Click **Actions > View Members**.
The Partitions > AppWorks Platform Partition dialog box opens.
10. Continue with Adding an OTDS User.

Adding an OTDS user

1. Click **Add > New User**.
The Users & Groups > AppWorks Platform Partition dialog box opens displaying the new user configuration fields.
2. Type the new **User ID**.
For example: ProcessAdmin

Note: This user ID and password must be the same as the user created during the AppWorks Platform installation. Refer to the Installation Worksheet for this information.

The following rules apply when creating a User ID:

- Can include upper and lowercase letters, numerals, blanks, and special characters.
- Cannot contain any reserved special characters, such as: `, + " \ < > ; = /`
- Cannot contain a blank or `#` at the beginning.
- Cannot contain a blank at the end.

3. Type values in other fields as needed. All other fields are optional. For example:
 - **First name** - Process
 - **Last name** - Admin
 - **Email** - ProcessAdmin@appworks.com
4. Click **Next**.
The Account Options configuration information for the new user is displayed.
5. For:

Do not require a password change on reset	Select this option.
User cannot change password	Select this option.
Password never expires	Select this option.
Password Confirm Password	Type a value.

6. Click **Next**.
The Organization dialog box opens.
7. Click **Next** as information is not required in this dialog box.
The User Attribute dialog box opens.
8. Click **Next**.
The Custom Attributes dialog box opens.
9. Click **Save** as information is not required in this dialog box.
The Partitions > AppWorks Platform Partition dialog box opens displaying the user just created.
10. Write the OTDS User name and Password on the Installation Worksheet.
The user is now created in OTDS.

Configuring AppWorks Platform for OTDS authentication

To enable single sign-on for the users across these products, you must integrate directory services such as Active directory, LDAP, and so on with OpenText Directory Services and register the OpenText products as resources to centralize the users.

This section includes:

- [Creating a resource for AppWorks Platform on page 62](#)
- [Configuring AppWorks Platform for OTDS authentication on page 65](#)

Creating a resource for AppWorks Platform

After the users are imported from Active Directory to OTDS or created in OTDS, you must create and activate resources for each component of the AppWorks. The following sections provide instructions to configure the resources of each component.

Important: The AppWorks Platform Hostname (server ID), port ID, user name and password values are required for this procedure.

To create and configure a user in AppWorks Platform:

1. Open the AppWorks Platform explorer.
2. Click **User Manager**.
The User Manager window opens.
3. Click **Add** (plus sign) on the toolbar.
The Create User page appears.
4. For:

Authentication type	Select Platform .
User Name	Type the unique name of the user.
Description	Type the description or the full name of the user.
User ID	Type the operating system identity of the user in the User ID field. This acts as a unique user identifier, which is used to sign in to the AppWorks Platform environment. If the User ID of an organizational user being created exists, you can map it to the existing authenticated user.
Default Organization	Select the default organization for the user.
Password	Expand Assign Password and type the password for the user and confirm it.

5. Click **Save**.
The user is created and displays on the Users pane.
6. Select **Include Internal Roles**.
The Roles pane on the right displays the available roles.
7. Click **Search** and type OTDS Push Service.
8. Right-click **OTDS Push Service** and select **Assign to selected Users**.
The OTDS Push Service role is assigned to the created user.

To create a resource for AppWorks Platform in OTDS:

1. Connect to OTDS server using the OTDS Web Administration and log on as Administrator.
The OTDS Administration page appears.

2. Click **Resources** on the navigation bar.
The Resources page appears.
3. Click **Add** (plus sign) to create a resource.
The New Resource page appears.
4. For:

Resource name	Type a descriptive name for this resource. For example: AppWorksPlatform
Display Name	Type the name for how you want this resource to be displayed.
Description	Optional. Type a description for this resource.
Login UI Version	Retain the default value.
Login UI Style	Leave the box empty.

5. Click **Next**.

Important: Do not click **Save**. Wait to save this resource until all parameters are configured.

The **New Resource > Synchronization** page appears.

6. For:

User and group synchronization	Select this check box.
Synchronization connector	Select Rest (Generic) connector from the list.
This connector will	Leave selected defaults: <ul style="list-style-type: none"> • Create users and groups • Modify users and groups <p>Note: OpenText recommends not selecting Delete users and groups operation in production environments.</p>

7. Click **Next**.

Important: Do not click **Save**. Wait to save this resource until all parameters are configured.

The **New Resource > Connection Information** page appears.

Note: See the Installation Worksheet for the AppWorks Platform information generated during the installation process. Use this information in the next step.

8. For:

Base URL	<p>Type the AppWorks Platform server URL to access AppWorks Platform.</p> <p>The URL comprises the protocol, host name, and port of the AppWorks Platform server, including the URL-encoded name of the organization to push to, and the fixed name of the push connector application, that is <code>otdspush</code>.</p> <p>For example:</p> <pre>http://<my appworks-platform-server.domain.com>/home/acme%20corp/app/otdspush</pre>
User Name	<p>Type the user name of the user created for OTDS push connector above.</p> <p>This user name is used to push users from OTDS to AppWorks Platform.</p>
Password	<p>Type the password of the user created during the AppWorks Platform installation.</p>

- Click **Test Connection** to verify that the details provided above are correct and a connection between AppWorks Platform and OTDS can be established.

When successful, a Connected Successfully message is displayed.

- Click **Next**.

The **New Resource > User Attribute Mapping** page appears.

- Accept the default values and click **Next**.

Note:

- If the page does not display any values, click **Reset to Default**. The New Resource > Group Attribute page appears.
- If you are integrating iHub with OTDS And AppWorks Platform, you must set the `_NAME_` parameter to **otExternalID03**.

- Accept the default values and click **Save** to create the resource.

Note: If the page does not display any values, click **Reset to Default**.

The Resource Activation – AppWorks Platform dialog opens displaying the resource identifier.

Important: Do not click **Verify Activation** because more configuration is required.

- Highlight and copy the resource identifier and paste it into a text editor or write this identifier on the Installation Worksheet so you can copy it later when configuring AppWorks Platform to use OTDS for authentication.
- Click **OK**.
The resource is created for AppWorks Platform.

Configuring AppWorks Platform for OTDS authentication

This section describes the steps for AppWorks Platform OTDS Authentication.

Topics include:

- [AppWorks Platform OTDS authentication on page 65](#)
- [AppWorks Platform trusted sites on page 66](#)

AppWorks Platform OTDS authentication

To configure AppWorks Platform OTDS Authentication:

1. Open a browser and access **AppWorks Platform Explorer > Security Administration > OTDS Resources > Platform**.
The Platform information is displayed.
2. In Shared Configuration, specify the values for the below fields:

OTDS Server URL	Type the URL to access the OTDS Server in the following format: <code>http://<computer name>:<port number></code> This must be a valid URL, starting with either http or https, for example: <code>http://server1:8080</code>
Resource ID	Enter the resource identifier of the AppWorks Platform resource created in OTDS.

Note: The Shared configuration can be used in all organizations. However, the Organization configuration can only be used in the current organization.

3. Click **Save**, and then click **Activate**.
A Notification page appears indicating the Resource was successfully activated.
4. Click **Close** on the message notification.
5. Click **Authenticators > Shared**.
The Authenticators tab appears.
6. Click **Add** (plus sign) on the Shared Authenticators table.
The Authenticator Details page appears.
7. For:

Id	Type an ID for the Authenticator. For example: OTDS
Default or Test Only	Select the Default check box.
Type	Select 'OTDS' from the list.

Note: Leave all other values or modify as needed.

8. The OTDS Properties tab is automatically populated with the OTDS resource information.
9. Optional. If the public URL of the OTDS server is different from the internal URL, for example when a proxy is used, then specify the Public OTDS login URL. Use the public URL of the OTDS server and concatenate `/otdsws/login`.
For example: `https://otds.acme.com:8443/otdsws/login`
10. Click **Save** and close the Security Administration page.
11. Continue with [AppWorks Platform trusted sites on page 66](#).

AppWorks Platform trusted sites

For authentication, the domain level URL for AppWorks Platform must be registered as trusted sites in OTDS to ensure that OTDS can redirect back to the products after the user has been authenticated. If you do not configure this, the following error message might occur after the user has been authenticated, and before returning to the originally requested application:

Not a trusted referral site, please contact your administrator.

To add a trusted site:

1. Open a browser and access **OTDS Admin** through `http://<hostname>:<tomcat port no>/otds-admin`.
The OTDS home page displays.
2. Click **Trusted Sites**.
3. Click **Add**.
4. Under **Addresses Directory Services will redirect requests to**, type the required URL in the format `<protocol>://<FQDN>:<AppWorksPlatformPort>`.
For example: `http://AppWorksPlatformServer.domain.suffix:81`
5. Click **Save**.
6. In the left frame, click **Access Roles**.
The Access Roles page appears.
7. Select **Access to AppWorksPlatform** and click **Actions > View Access Role Details**.
The **Access to AppWorksPlatform > User Partitions** tab page appears.
8. Click **Add**.
The **Add Partitions – Access to AppWorksPlatform** page appears.

9. Select the **AppWorksPlatform Partition** that was previously created and click **Add Selected Items to Access Role**.
10. Click **Close Dialog** to close the page.
11. Click **Save**.
The page is refreshed.

Note: Adding the User Partition automatically pushes all the users and groups to AppWorks Platform. Users in OTDS are pushed as authenticated users to AppWorks Platform and groups in OTDS are pushed as roles to AppWorks Platform.

12. **Optional:** If you have multiple partitions added to Access Roles, select the **Access to AppWorksPlatform** role and click **Actions > Include Groups from OUs**.
The Include/Exclude Groups from OUs message displays.

13. Click **OK**.
The Access Roles page refreshes showing this selection is now included.

14. Close this page.

Note: To push the AppWorks Platform package roles to OTDS, use the OTDS Push roles functionality available in Security Administration. For more information, see the Synchronizing roles from AppWorks Platform to OTDS topic in the *AppWorks Platform Administration Guide*.

Configuring OTDS authentication for an organization

Follow these steps to configure OTDS authentication for each organization:

- [Creating a user to push users and groups into AppWorks Platform on page 68](#)
- [Creating an organization-specific partition for groups and roles on page 69](#)
- [Creating an organization-specific resource for AppWorks Platform in OTDS on page 69](#)
- [Linking the organization-specific partition to the organization-specific resource on page 72](#)
- [Synchronizing roles on page 73](#)
- [Creating a process administrator user on page 73](#)
- [Managing users and group membership for a specific organization on page 74](#)
- [Consolidating a resource on page 75](#)
- [Verifying the configuration on page 76](#)

Note: This section assumes that the name of the organization is System.

Creating a user to push users and groups into AppWorks Platform

The push connector runs in OTDS and connects to AppWorks Platform to sync users. This must be done under a user context that is allowed to do so. Therefore, we must create a user in AppWorks Platform with a specific role and configure this user in the OTDS REST push connector.

To create and configure a user for the OTDS push connector:

1. Open a browser and access AppWorks Platform Explorer.
2. Click **User Manager**.
The User Manager window opens.
3. Click **+** (Add a User) on the toolbar.
The Create User page appears.
4. For:

Field	Value
Authentication Type	Select Platform .
User Name	Type the unique name of the user. For example: JDoe
User Full Name	Type the full name of the user. For example: John Doe
User ID	Type the operating system identity of the user in the User ID field. This acts as a unique user identifier, which is used to sign in to AppWorks Platform. Note: If the User ID of an organizational user being created already exists (because you have set up another organization already), you can map it to the existing authenticated user in the dialog box that pops up.
Password	Type the password for the

Field	Value
	user.
Confirm Password	Confirm the password.

5. Click **Save**.
The user name displays on the Users pane.
6. Click the user to select.
The selected user name is highlighted.
7. Select Include Internal Roles.
The Roles pane on the right displays the available roles.
8. On the Roles pane, click **Search** and type **OTDS Push Service**.
9. Right-click OTDS Push Service, and then select **Assign to selected User(s)**.

The OTDS Push Service role is assigned to the created user.

Creating an organization-specific partition for groups and roles

To create an organization-specific partition for groups and roles:

1. Launch a browser and type the following URL:
`http://<hostname>:<tomcat port no>/otds-admin`
For example:
`http://localhost:8080/otds-admin`
2. Sign in with appropriate credentials.
Tip: Retrieve this user name and password from the Installation Worksheet or contact your system administrator.
The OTDS Administration page appears.
3. Click **Partitions**.
The Partitions page appears.
4. Click **Add > New Non-synchronized User Partition**.
5. Type a name, for example: AppWorks Platform Groups for System, and then click **Save**.
The partition is added.

Creating an organization-specific resource for AppWorks Platform in OTDS

Important: During resource creation, click **Save** after all the parameters are configured and you are prompted to save. When you click Save, OTDS schedules a synchronization

task. Therefore, synchronizing a resource without completing the required configurations might result in duplicate or lost data in AppWorks Platform.

To create a resource for AppWorks Platform in OTDS:

1. On the OTDS Administration page, click **Resources** on the navigation bar.
The Resources page appears.
2. Click **Add** (plus sign) to create a resource.
The New Resource page appears.
3. For:

Resource name	Type a descriptive name for this resource. For example: AppWorks Platform Resource for System
Display Name	Type the name by which the resource displays.
Description	Optional. Type a description for this resource.
Sign in UI Version	Retain the default value to accept the default value of the resource.
Sign in UI Style	Leave the box empty.
Sign out URL	Leave the box empty.
Sign out Method	Leave the box empty.

4. Click **Next**.

Important: Do not click **Save**. Wait to save this resource until all parameters are configured.

The New Resource > Synchronization page appears.

5. For:

User and group synchronization	Select this check box.
Synchronization connector	Select Rest (Generic) connector from the list.
This connector will	Leave selected defaults: <ul style="list-style-type: none"> • Create users and groups • Modify users and groups <p>Note: OpenText recommends not selecting Delete users and groups operation in production environments.</p>

6. Click **Next**.

Important: Do not click **Save**. Wait to save this resource until all parameters are configured.

The New Resource > Connection Information page appears.

Note: Refer to the Installation Worksheet for the AppWorks Platform information generated during the installation process. Use this information in the next step.

7. For:

Base URL	Type the AppWorks Platform server URL to access AppWorks Platform. The URL comprises the protocol, host name, and port of the AppWorks Platform server, including the (URL encoded) name of the organization to push to, and the fixed name of the push connector application (otdspush). For example: <code>http://<my appworks-platform-server.domain.com>/home/acme%20corp/app/otdspush</code>
User Name	Type the user name of the user created for the OTDS push connector. For example: JDoe This user name is used to push users from OTDS to AppWorks Platform.
Password	Type the password of the user created during the AppWorks Platform installation.

8. Click **Test Connection** to verify that the details provided are correct and a connection between AppWorks Platform and OTDS can be established.

When successful, a Connected Successfully message displays.

9. Click **Next**.

The New Resource > User Attribute Mapping page appears.

10. Accept the default values and click **Next**.

Note: If the page does not display any values, click **Reset to Default**.

The New Resource > Group Attribute page appears.

11. Accept the default values and click **Save** to create the resource.

Note: If the page does not display any values, click **Reset to Default**.

The Resource Activation – AppWorks Platform dialog box displays the resource identifier.

Important: Do not click **Verify Activation** because more configuration is required.

12. Highlight and copy the resource identifier and paste it into a text editor or write this identifier on the Installation Worksheet so you can copy it later when configuring AppWorks Platform to use OTDS for authentication.
13. Click **OK**.
The resource is created for AppWorks Platform.

Linking the organization-specific partition to the organization-specific resource

To provide users access to an organization, you must link them to the organization-specific resource. This can be achieved in multiple ways, but the preferred way is to add the entire organization-specific partition (AppWorks Platform Groups for System) created above to the access role of the System organization.

To link the partition to the access role:

1. Launch a browser and type the following URL:
`http://<hostname>:<tomcat port no>/otds-admin`
For example:
`http://localhost:8080/otds-admin`
2. Sign in with appropriate credentials.
Tip: Retrieve this user name and password from the Installation Worksheet or contact your system administrator.
The OTDS Administration page appears.
3. Click **Access Roles** on the navigation bar.
The Access Role page appears.
4. In the table, find the Access to AppWorks Platform Resource for System access role.
5. Click **Actions**, and then select Include groups if they are not included.
6. Click **OK** in the confirmation dialog box that opens.
7. Click **Actions > View Access Role Details**.
The Access Role Details page appears.
8. Navigate to the **User Partitions** tab, and then click **Add**.
The Add Partitions - Access to AppWorks Platform Resource for System window opens.
9. Search for the AppWorks Platform Groups for System partition, select it, and then click **Add Selected Items to Access Role**.
10. Click **Close Dialog**, and then click **Save**.

Synchronizing roles

This topic describes the procedure to synchronize AppWorks Platform package roles with OTDS. Functional and application roles from packages that are available in the shared space and in the specified organization context are created in OTDS.

The package roles in AppWorks Platform are created in the `<Package Name>#<Role Name>` format, for example, `Case Management#Case Worker`.

To synchronize roles from AppWorks Platform to OTDS:

1. On the **Welcome** page, click **Security Administration**.
The Security Administration window opens and the **Certificates** tab is displayed by default.
2. Click the **OTDS Resources** tab.
3. Click the **OTDS Push Roles** tab.
The OTDS push role page opens and the OTDS server URL is prefilled from the configured Platform resource.
4. Type a name for the OTDS partition in OTDS partition name. If the partition does not exist in OTDS, then a non-synchronized user partition is created.
5. Optional. Select **Delete roles** if you want the package roles not found in AppWorks Platform to be deleted from OTDS.
6. Click **Save** to save the configuration.
7. Click **Push roles**.
The status field displays the progress of the role synchronization. You can click **Refresh** to obtain the latest status and to see if the role synchronization is complete.

Note: The OTDS role push functionality cannot detect a role name change. Therefore, when a role is renamed, the user and group membership of that role is lost. You must map the role to the user and group membership again.

Creating a process administrator user

Create a user and link the user to the partition that was created above.

To create a process administrator user:

1. Launch a browser and type the following URL:
`http://<hostname>:<tomcat port no>/otds-admin`
For example:
`http://localhost:8080/otds-admin`
2. Sign in with appropriate credentials.

Note: Retrieve this user name and password from the Installation Worksheet or contact your system administrator.

The OTDS Administration page appears.

3. Click **Partitions**.
The Partitions page appears.
4. Find the AppWorks Platform Groups for System partition.
5. Click **Actions > View Members**.
A page appears with a list of users.
6. Click **Add > New User**.
The new user page appears.
7. Type the user name as ProcessAdmin, and then click **Save**.
The user is created and added to the partition.
8. Click **Actions > Edit Membership**.
The Member Of page appears.
9. Click **Add To Group**.
The Users and Groups Associations dialog box opens.
10. Search for Cordys@Work#Administrator, select the corresponding group for the user partition AppWorks Platform Group for System, and then click **Add Selected**.

The ProcessAdmin user is assigned to the Cordys@Work#Administrator group.

Managing users and group membership for a specific organization

You can add users and groups to the System organization using the AppWorks Platform Groups for System partition.

- Adding a user to a group in the partition.
- Adding a group to another group in the partition.

Important: Open Text recommends that you do NOT add a user to the access role directly. If there is a requirement to have additional users in AppWorks Platform without any role in an organization, you can follow the steps below to add a user to an access role. However, to simplify and reduce the overhead, do the following:

1. Create an extra group called Guest users in the partition AppWorks Platform Groups for System (which is part of the access role already).
2. Add the users not having a role in AppWorks Platform to that group.

To add a user or group to a group:

1. Launch a browser and type the following URL:
`http://<hostname>:<tomcat port no>/otds-admin`
For example:
`http://localhost:8080/otds-admin`

2. Sign in with appropriate credentials.

Note: Retrieve this user name and password from the Installation Worksheet or contact your system administrator.

The OTDS Administration page appears.

3. Click **Partitions**.
The Partitions page appears.
4. Find the AppWorks Platform Groups for System partition.
5. Click **Actions > View Members**.
A page appears with a list of users.
6. Click the **Groups** tab.
A page appears with a list of groups.
7. Find the group to add members, and then click **Actions > Edit Membership**.
The membership page appears, showing a list of all current members.
8. Click **Add Member**.
The Users and Groups Associations dialog box opens.
9. Search for required users in the AppWorks Platform Groups for System partition. For example, John Doe.
10. Select the user, and then click **Add Selected** on the toolbar.
11. Similarly, you can repeat the above step for groups.
Note: Ensure that you select the groups from the AppWorks Platform Groups for System only.
12. After adding all users and groups, click **Close** to close the dialog box.

Consolidating a resource

When a change is made to a user, group, or resource, it must automatically be pushed to AppWorks Platform. If the users are not automatically pushed to AppWorks Platform, or you want to ensure that the changes are pushed, you can consolidate a resource.

To consolidate a resource:

1. Launch a browser and type the following URL:
`http://<hostname>:<tomcat port no>/otds-admin`
For example:
`http://localhost:8080/otds-admin`
2. Sign in with appropriate credentials.

Note: Retrieve this user name and password from the Installation Worksheet or contact your system administrator.

The OTDS Administration page appears.

3. Click **Resources** on the navigation bar.
The Resources page appears.
4. For the AppWorks Platform Resource for System resource, click **Actions** > **Consolidate**.
5. Click **Consolidate**.
The consolidation is triggered. The time taken to consolidate depends on the number of users and groups. Consolidation checks every user and group, and pushes updates to AppWorks Platform.

Verifying the configuration

After all the configurations are complete, you can verify the configuration.

To verify the configuration:

1. Open a browser and type the AppWorks Platform URL.
2. Sign in with the credentials of the existing user.

OTDS authentication is configured. When users open AppWorks Platform, they are redirected to OTDS to sign in.

Disabling the authentication handler

You must disable the `http.negotiate` authentication handler because Kerberos authentication is not being used.

To configure authentication handlers:

1. Open a browser and access OTDS Admin through `http://<hostname>:<tomcat port no>/otds-admin`.
The OTDS home page is displayed.
2. Select **Authentication Handlers**.
3. Select **http.negotiate** > **Actions** > **Disable**.

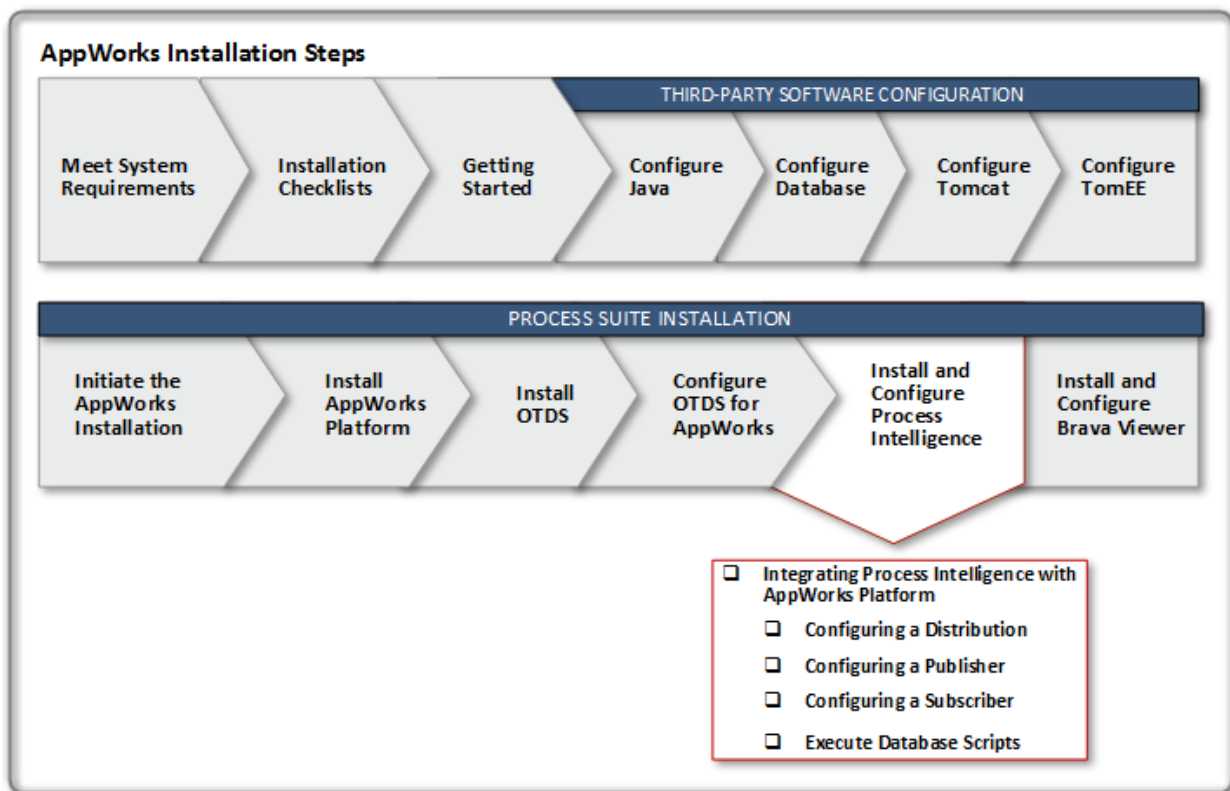
The window refreshes, showing `http.negotiate` is disabled.

Chapter 10

Installing and configuring Process Intelligence

This section identifies the installation of Process Intelligence and its integration with AppWorks Platform.

Note: Installation of Process Intelligence is optional.



After completing OpenText Directory Services installation, you can continue with Process Intelligence server installation.

See the Process Intelligence Installation Guide on [My Support](#) for installation instructions for various scenarios. The following section provides instructions based on a standalone installation:

Before you begin:

- Ensure that all the [System requirements on page 10](#) are met.
- Ensure that the following Windows services are run as Administrator:
 - SQL Server
 - Server Analysis Services
- If you use IIS 7.0/7.5/8.0/8.5, ensure that IIS is enabled and the following role services are installed:
 - ASP.NET
 - Windows Authentication
 - Basic Authentication
 - IIS 6.0 Management Compatibility

See [Configuring IIS on page 116](#) for configuration details.

- If you use IIS 6.0, ensure that the ASP.NET 2.0 web extension is installed and enabled.

To install Process Intelligence:

1. Navigate to <extracted_installdir>, right-click **Mastersetup.exe** and select **Run as Administrator**.
The AppWorks Installer dialog box opens.
2. Click **Run**.
The AppWorks Installer page appears.
3. Click **Next**.
The License Agreement page appears.
4. Review the license agreement carefully by scrolling to the bottom of the agreement. Select the **I accept the terms in the License Agreement** check box, and click **Agree**.
The Deployment Scenarios page appears.
5. Select the **OpenText Process Intelligence** check box, and then click **Next**.
The Product Groups dialog box opens with Product Groups and Components collapsed.
6. Expand the OpenText Process Intelligence group and select **OpenText Process Intelligence**.
7. Click **Next**.
The Summary page displays the component you selected.
8. Verify that the component from the previous step is shown and click **Install**.
The InstallAnywhere wizard is initiated and displays a Welcome page.
9. Click **Next**.
The Choose Destination Location page appears.

10. Type the path to install Process Intelligence Server or click **Browse** to select a folder location.

By default, the Process Intelligence components are installed at: C:\Program Files\OpenText\Process Intelligence.

11. Click **Next**.
The Select Features page appears.
12. Select all components.

Server Administration	Installs Server Administration.
Analysis Engine	Installs the Analysis Engine. You cannot run multiple instances of the Analysis Engine against the same relational database. Installation packages for the Adapter Service and the Translator Service for SQL Server are also copied together with the Analysis Engine installation.
Integration Service	Installs the Integration Service.
Databases	Installs the relational and OLAP databases. You can install the databases during any installation run.

13. Click **Next**.
The Ready to Install the Program page appears.
14. Click **Install**.
The Setup Status window opens.
15. When the process is complete, continue with Configuring the databases.

Configuring the databases

The Database Configuration page appears if you selected **Databases** on the Select Features page.

By default, Process Intelligence creates both relational and OLAP databases. However, from Process Intelligence 16.1 release, it is optional to use the OLAP database.

Therefore, if your application does not need analysis databases, clear the **Install OLAP Database** option. In such instances, skip steps 6-7 in the following procedure:

To configure the relational and OLAP databases:

1. Click **Next**.
The Relational Database Configuration page appears.
2. Select or enter a server name that is either the Host name or the DNS name of the server.
If you want to specify a SQL Server named instance, you must use the following format:
`<server name>\<instance name>`
3. **Optional:** If you want to use a separate staging database, select **Use separate Staging database**. See the Configuring Relational Database topic in the Process Intelligence installation guide on [My Support](#).
4. Select **Create Database**.
5. **Optional:** If you selected the **Use separate Staging database** option, the Staging Database Install page appears. Provide the required details and click **Next**. See the Configuring the staging database topic in the Process Intelligence installation guide on [My Support](#) for information on the inputs to be provided.
Note: If the **Install OLAP Database** option is NOT selected on the first screen of this procedure, the screens in steps 6-7 do not display. You can skip the steps 6-7 and continue with step 8.
6. Click **Next** to create the respective database.
The OLAP Database Configuration dialog box opens.
7. Enter the following information:

Analysis Services Server Name	Name of the instance of the Microsoft SQL Analysis Services that contains the OLAP database in the Analysis Services Server Name field.
OLAP Database Name	Name of the OLAP database. The default name is AEOLAP.

8. Click **Next** to create the database.
The Database Configuration page displays.
9. Click **Finish**.
The InstallShield wizard displays the completion message.
10. Click **Finish** to exit the wizard.

Verifying the installation

After you configure the database, you must verify the installation on the Process Intelligence computer.

To verify the installation on the Process Intelligence computer:

- Verify that the Process Intelligence directory is installed at the location you specified during the installation. The default installation directory is: `C:\Program Files\OpenText\Process Intelligence`.
- The Process Intelligence directory contains a subdirectory for each installed feature. If you installed all features on a single computer, the Process Intelligence directory includes the following subdirectories:
 - Admin
 - Analysis Engine
 - Integration
 - Integration Service
 - Shared
- Open a web browser and enter Server Administration URL.
The default URL is: `http://<Server name>\ProcessIntelligenceAdmin\Management.aspx`

Alternatively, you can use the Start menu shortcut: **OpenText > Process Intelligence Server > Process Intelligence Server Administration**

The Server Administration page appears.

Verify the following:

Controls & Monitoring > Published Records	The row counts for each of the Process Intelligence Statistics categories is zero. This indicates that Server Administration can connect to the databases. The row counts must be zero until you send data through Process Intelligence.
Controls & Monitoring > Analysis Engine	The Analysis Engine can be started and stopped successfully. Click Start and Stop to start and stop the Analysis Engine respectively.
Management > About Process Intelligence	The databases are installed at the intended location and the Process Intelligence version number is correct.

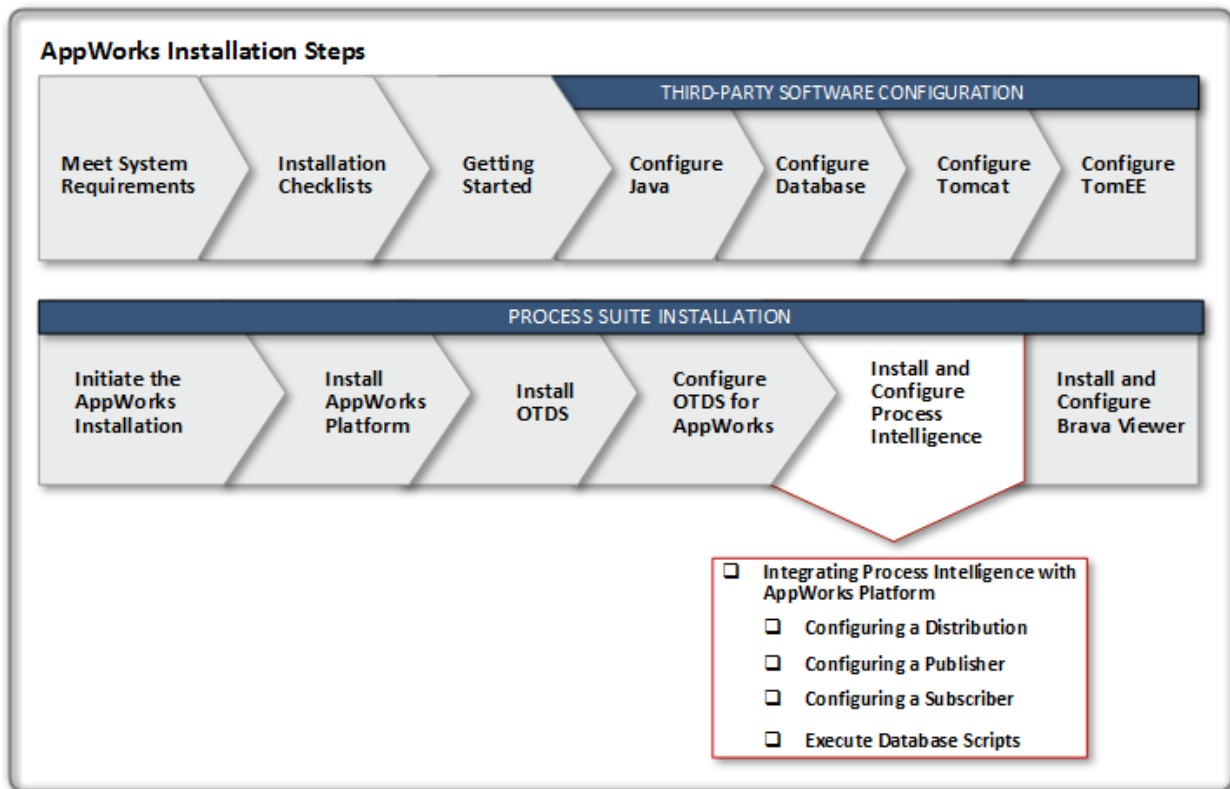
- Access Microsoft SQL Server Management Studio to verify that the Process Intelligence databases are displayed.
 - The default name of the relational database is AEDB.
 - The default name of the OLAP database is AEOLAP.
- Use Server Administration to process your Statistics cubes.

- Verify that the Integration Service is installed correctly.
Open a web browser and enter the Integration Service URL. The default URL is:
`http://<Server name>/ProcessIntelligenceIntegration/IntegrationService.svc`

Integrating Process Intelligence with AppWorks Platform

This section identifies the integration of Process Intelligence with AppWorks Platform.

Note: Installation of Process Intelligence is optional.



After completing [Installing and configuring Process Intelligence on page 77](#), integrate it with AppWorks Platform.

Note: To perform this task, ensure that the SQL Server Replication option is selected. If you cannot see the Replication folder as specified in the procedures below, contact your system administrator to install the SQL Server Replication feature.

The following are the basic steps to integrate Process Intelligence with AppWorks Platform:

- [Configuring a distribution on page 83](#)
- [Configuring a publisher on page 83](#)

- [Configuring a subscriber on page 88](#)
- [Disabling publishing and distribution on page 89](#)
- [Running database scripts on page 91](#)

The following sections describe each step in detail. Follow the procedures in this order:

Configuring a distribution

Configure distribution on the servers where AppWorks Platform and Process Intelligence are installed.

Prerequisite:

Ensure that the SQL Server Agent is started.

To configure a distribution:

1. Connect to the Publisher in SQL Server Management Studio, and expand the server node.
2. Right-click the **Replication** folder and click **Configure Distribution**.

The Configure Distribution Wizard page appears.

Note: If you connected to SQL Server using localhost rather than the actual server name, you are prompted with a warning that SQL Server is unable to connect to server `localhost`. Click **OK**. In the Connect to Server page, change the Server name from `localhost` to the name of your server and then click **Connect**.

3. Click **Next**.
The Distributor page appears.
4. On the Distributor page, select **<server name> will act as its own Distributor**.
SQL Server creates a distribution database and log.
5. Click **Next**.
6. In the Snapshot folder text box, retain the default location, and click **Next**.
The Distribution Database page appears.
7. Accept the default values on the remaining pages of the wizard and click **Finish** to enable distribution.
8. Click **Close** to exit the window.

Configuring a publisher

Create a publisher on the server where AppWorks Platform is installed and set database permissions as publisher for the AppWorks Platform database.

To configure a publisher:

1. In SQL Server Management Studio, expand **Replication**, right-click **Local Publication**, and then select **New Publication**.

The New Publication Wizard opens.

2. Click **Next**.
The Publication Database page appears.
3. Select the **<AppWorks Platform database>** and click **Next**.
The Publication Type page appears.
4. Select **Transactional Publication**, and click **Next**.
The Articles page appears.
5. Expand **Tables** and select the following Tables/Columns to be used as publisher articles.

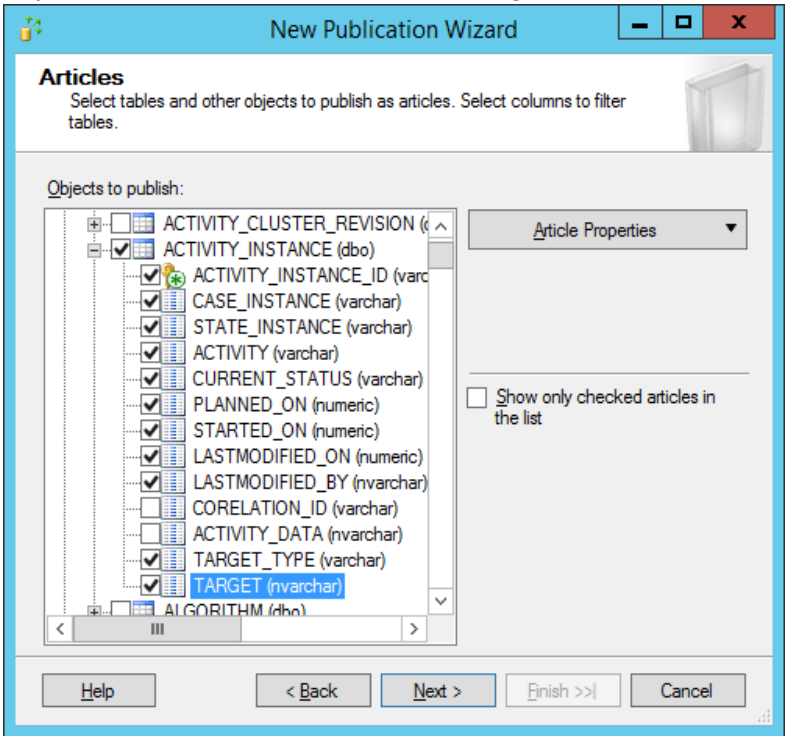


Table	Columns
ACTIVITY_INSTANCE	ACTIVITY_INSTANCE_ID CASE_INSTANCE STATE_INSTANCE ACTIVITY CURRENT_STATUS PLANNED_ON STARTED_ON LASTMODIFIED_ON LASTMODIFIED_BY

Table	Columns
	TARGET_TYPE TARGET
BPM_MODEL	All Columns
BPM_MODEL_REVISION	REVISION_ID MODEL_ID CREATED_ON
BUSINESS_IDENTIFIER	All Columns
BUSINESS_IDENTIFIER_DATE	All Columns
BUSINESS_IDENTIFIER_NUMERIC	All Columns
BUSINESS_IDENTIFIER_REVISION	All Columns
BUSINESS_IDENTIFIER_STRING	All Columns
CASE_ACTIVITY	ACTIVITY_ID ACTIVITY_MODEL_ID STATE CLUSTER_NAME ACTIVITY_NAME ACTIVITY_TYPE
CASE_INSTANCE	CASE_INSTANCE_ID CASE_MODEL MODEL_REVISION ROOT_ID ROOT_TYPE SOURCE_TYPE SOURCE DUE_ON STARTED_ON LASTMODIFIED_ON STARTED_BY LASTMODIFIED_BY STATUS ORGANIZATION TARGET PRIORITY

Table	Columns
CASE_INSTANCE_IDENTIFIERS	All Columns
CASE_MODEL_IDENTIFIER	All Columns
NOTF_TASK_INSTANCE	TASK_INSTANCE_ID TARGET PARENT_TASK_ID HUMAN_TASK_ID TASK_OWNER SOURCE_NAME ACTIVITY_ID SOURCE_INSTANCE_ID SOURCE_TYPE SUBJECT STATE TASK_INFO ROOT_CASE_INSTANCE_ID
PARTICIPANT	PARTICIPANT_ID DISTINCT_NAME
PROCESS_ACTIVITY	INSTANCE_ID ACTIVITY_ID ITERATION_COUNT REPLACED ACTIVITY_INSTANCE_ID PARENT_ID ACTIVITY_NAME ACTIVITY_TYPE STATUS START_TIME END_TIME PARTICIPANT EXECUTED_BY
PROCESS_INSTANCE	INSTANCE_ID PARENT_ID PARENT_TYPE ROOT_ID

Table	Columns
	ROOT_TYPE MODEL_ID MODEL_REVISION_ID PROCESS_NAME START_TIME END_TIME VERSION DESCRIPTION TYPE USER_NAME ORGANIZATION CURRENT_OWNER PROCESS_TYPE PROCESS_PRIORITY STATUS IS_ARCHIVED PUBLISHED_TO RUNTIME_DOCUMENT_ID

6. Click **Next**.
The Filter Tables Rows page appears.
7. Click **Next**.
The Snapshot Agent page appears.
8. Select the following options:
 - Create a snapshot immediately and keep the snapshot available to initialize subscriptions
 - Schedule the Snapshot Agent to run at the following times:
9. Click **Next**.
The Agent Security page appears.
10. Click **Security Settings**.
The Security Settings page appears.
11. Select one of the following options:
 - If you want to use a Windows account, select **Run** under the following Windows account check box and provide the relevant details.

- If you want to use an SQL Server Agent account, such as an `sa` account, select **Run** under the SQL Server Agent account option.
12. Click **OK**.
The Agent Security page is populated, as shown in the following example.
 13. Click **Next**.
The Wizard Actions page appears.
 14. Select **Create the Publication** option and click **Next**.
The Complete the Wizard page appears.
 15. Type a name for the publication and click **Finish**.
The publisher is configured.

The New Publication Wizard page appears. It displays the status of the configuration process.
 16. Click **Close** to exit the wizard.

Configuring a subscriber

Configure a subscriber on the server where Process Intelligence is installed and select AEDB as the publisher.

To configure a subscriber:

1. In SQL Server Management Studio, expand **Replication**, right-click **Local Subscriptions**, and select **New Subscription**.

The New Subscription Wizard starts.

2. Click **Next**.
The Subscription database page appears.

3. For:

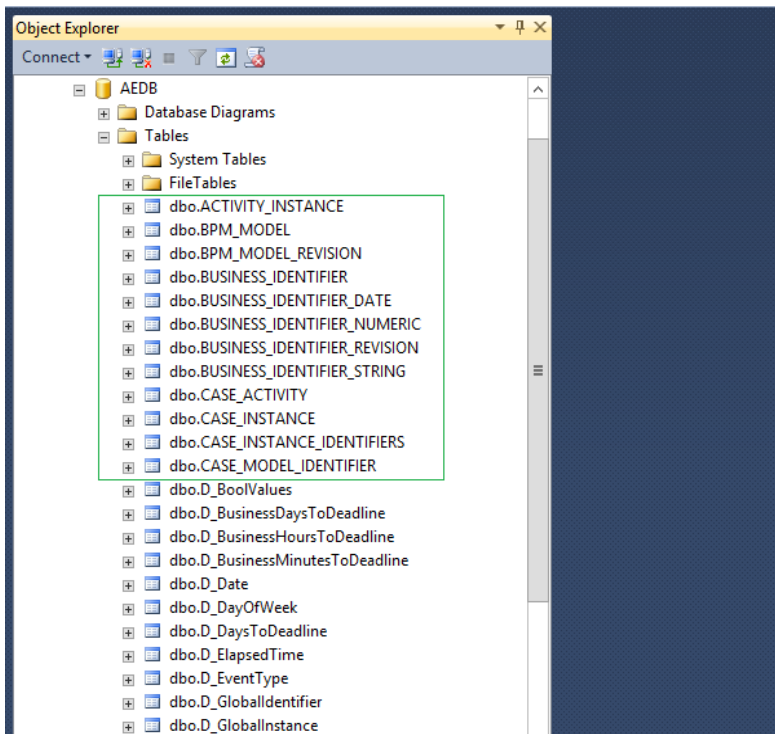
Publisher	Select the server where AppWorks Platform is installed.
Databases and publications	Select the publisher that was previously defined.

4. Click **Next**.
The Distribution Agent Location page appears.
5. Select **Run all at all Distributor, <server name> (push subscriptions)** and click **Next**.
The Subscribers page appears.

6. Select the instance name of the subscriber server, and select **AEDB** under Subscription Database.
7. Click **Next**.
The Distribution Agent Security page appears.
8. Click the **ellipsis (...)** button and do the following:

Process account	Enter <code>Domain\Account</code>
Password	Enter the password for the account.

9. Click **Finish** to accept the default values on the remaining pages and complete the wizard.
The subscriber is configured.
10. Verify that the tables are created in the database as follows.



Disabling publishing and distribution

If you deleted the replication configuration and want to reconfigure, ensure that you disabled the distribution before you start the configuration process.

To disable the distribution:

1. In SQL Server Management Studio, right-click **Replication** and select **Disable Publishing and Distribution**.
The Disabling Publishing and Distribution Wizard opens.
2. Click **Next**.
The Disable Publishing page appears.
3. Select the **Yes, disable publishing on this server** option and click **Next**.
The Complete the Wizard page appears.
4. Click **Finish**.
The Disabling Distribution page appears.
5. Click **Close**.
6. Repeat the instructions provided in the topic to reconfigure the replication process.

Running database scripts

The required database scripts are available at the following location:

```
<AppWorks Platform_  
installldir>/components/bpmengine/database/processintelligence/createscripts
```

Run the scripts in the AEDB database in this sequence:

1. PI_MSSQL_FUNCTIONS.sql
2. PI_MSSQL_PROCEDURES.sql
3. PI_MSSQL_TRIGGERS.sql

Note: By default, these scripts run in the SQL Server database default schema, which is `.dbo`. However, if the tables are created on a different schema, ensure that you add the schema to every table before running these scripts.

Integrating Process Intelligence with iHub

OpenText Information Hub (iHub) can connect to the Process Intelligence database to display information through reports and dashboards built in OpenText Analytics Designer. To get started quickly, an Analytics Designer project is provided which contains dashboards, reports, measures, and hierarchies. The sample dashboards and reports can directly be used with Process Intelligence. These can also be customized using the available measures and hierarchies.

See Process Intelligence iHub Integration Guide on [My Support](#), which contains details about the sample content and provides instructions for using the Analytics Designer project to build reports and dashboards that connect to the Process Intelligence.

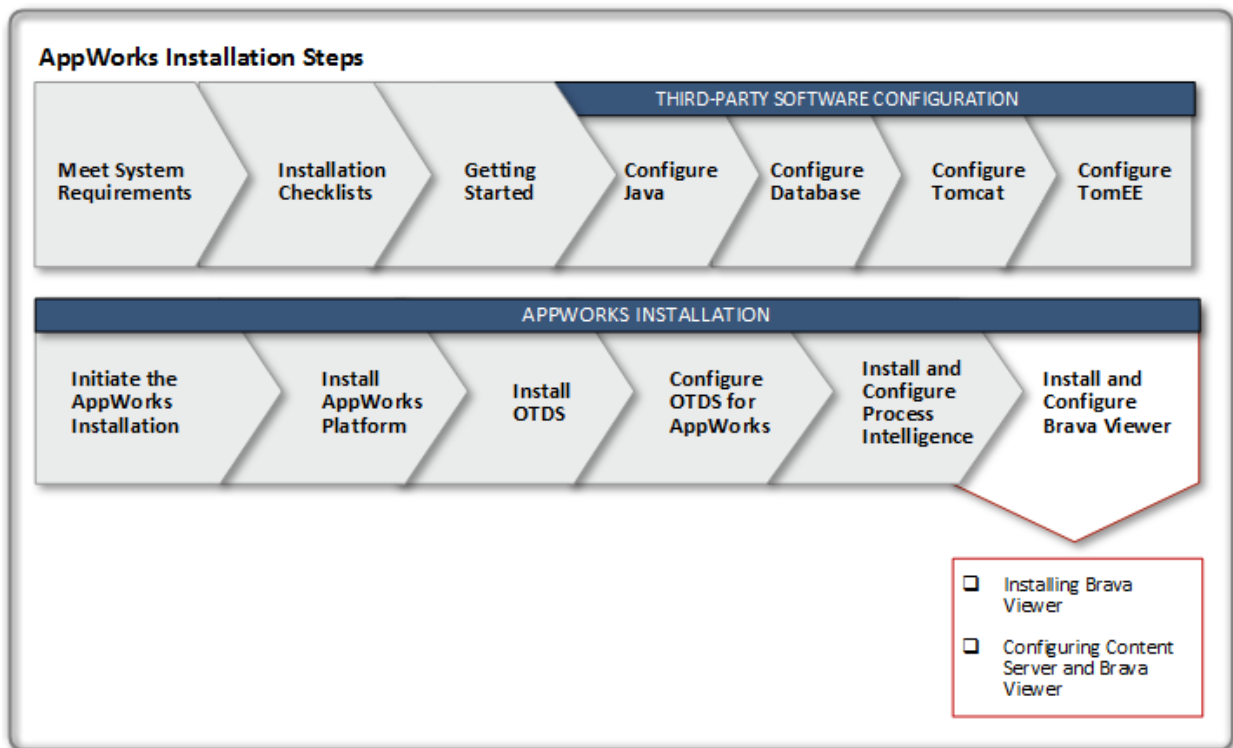
Chapter 11

Installing and configuring Brava

This section describes the installation and configuration of Brava with AppWorks Platform.

The Brava Viewer that is bundled with AppWorks is read-only and supports viewing and comparing of files. The file types supported are: BMP, JPEG, PNG, TIFF, PDF, and MS Office documents.

Note: Installation of Brava Enterprise is optional. The Brava Viewer functionality differs from the full functionality of the unrestricted versions of Brava. Contact your OpenText customer support for additional information.



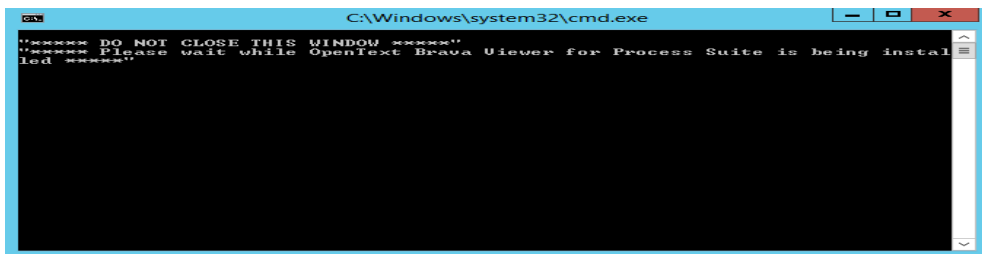
Before you begin:

Ensure that the user installing Brava has administrative privileges.

Installing Brava Enterprise

To install Brava Enterprise:

1. Navigate to <extracted_installdir> and double-click **Mastersetup.exe**.
The OpenText AppWorks Installer page appears.
2. Click **Next**.
The License Agreement page appears.
3. Review the license agreement carefully by scrolling to the bottom of the agreement. Select the **I accept the terms in the License Agreement** check box, and click **Agree**.
The Deployment Scenarios page appears.
4. Select the **OpenText Brava** check box, and click **Next**.
The Product Groups dialog box opens with Product Groups and Components collapsed.
5. Expand the OpenText Brava group and select **OpenText Brava Viewer**.
6. Click **Next**.
The Summary page appears with the selected component.
7. Click **Install**.
A Command Prompt window opens and runs in the background. Do not close this window.



The InstallAnywhere wizard is initiated and displays a Welcome page.

8. Click **Next**.
The License Agreement page appears.
9. Select **I accept the terms in the license agreement** and click **Next**.
The destination folder page appears.
10. Retain the default location and click **Next**.
The custom setup page appears.
11. Retain the default selections and click **Next**.
The Tomcat port settings page appears.
12. Retain the default values and click **Next**.

Note: Brava runs on Tomcat default port (8080) only. So, if you are installing Brava on a server that has other products using Tomcat, ensure that the default Tomcat port number 8080 is allocated only to Brava.

The Brava server settings page appears.

13. Retain the default values and click **Next**.

The service user information page appears.

14. Do the following:

User name	Type the appropriate user name in the correct convention: <Domain>\<User name> or do the following: <ol style="list-style-type: none"> a. Click Browse. The Browse for User name dialog box opens. b. Click Browse next to Domain or Server field. c. From the Select Domain or Server list, select the relevant option. d. From the Select User Name list, select the appropriate name. Ensure that the user name is in the <Domain>\<User name> format.
Password	Type a password for this user.

15. Click **Next**.

The License server settings page appears.

16. Click **Next**.

The SMTP server settings page appears.

17. Click **Next**.

The Ready to Install the Program page appears.

18. Click **Install**.

The installation progress screens appear and the InstallShield Wizard Completed page appears.

19. Click **Finish**.

The Command Prompt window opens.

20. Type `y` for Have you installed Brava JobProcessor in this machine [Y/N]?

21. Type the full directory path for Enter the full directory path of JobProcessor, for example, `C:\Program Files <86>\IGC\Brava! Enterprise\JobProcessor`

22. Type the full directory path for Enter the full directory path of Brava! License, for example, `C:\Program Files <86>\IGC\Brava! Enterprise\Brava! License`

23. Press any key to exit.

Brava Viewer installation is complete.

24. Continue with [Configuring Brava Viewer with AppWorks Platform on page 95](#).

Configuring Brava Viewer with AppWorks Platform

To view documents stored in the Document Management System (DMS), configure Brava Viewer with the document store service container. The repository service container is the default document store service container provided by AppWorks Platform. This service container is configured for the AppWorks Platform repository.

You can change this default behavior by specifying that your DMS is the document store service container.

The following procedure describes the configuration of Brava Viewer with the default Repository service container.

To configure Brava Viewer with AppWorks Platform:

1. Navigate to the AppWorks Platform explorer and access the System Resource Manager.
2. Double-click the Repository service container.
The Property-Repository pane opens.
3. Click **Document Store** and type the following in the Brava Server URL field:
`http://<Brava hostname>:<port number>`
4. Click **Save**.
5. Right-click the Repository service container and select **Restart**.
6. After the service container is restarted, open the web browser and type the following URLs:
 - `http://<AppWorks Platform host name>:<TomEE port number>/home/<organization name>/app/document services/rest/cache/reset`
 - `http://<AppWorks Platform host name>:<TomEE port number>/home/<organization name>/app/document services/rest/cache/flushOrgEntry`

Brava Viewer is installed and configured for AppWorks Platform.

Appendix A

High availability

An enterprise system is highly available when it is designed to be resilient to various disruptions that can happen in the system, and their dependent resources and infrastructure. These may include system crashes, application crashes, network problems, and so on. High availability ensures continuous availability of application services to the end users and uninterrupted business. Lack of high availability not only causes disrupted service, but also loss of business and damage to the reputation of the business provider. The high availability of systems has gained tremendous importance and prominence due to globalization, Internet revolution, an increasing community of online users, and greater dependence on the shared software services across geographical locations.

Business providers want their businesses to grow through continuous expansion of their customer base. Therefore, in addition to being highly available, the software must also be scalable to meet the growing needs of the business and its customers, without affecting performance.

AppWorks is built for high availability and scalability. Achieving high availability requires a cluster of computers (nodes) that work together to ensure that services running within the cluster never stop operating.

Before setting up high availability for AppWorks, ensure that you have administrative privileges on the computers where you want to configure AppWorks. You must also have experience working with networked computers and a working knowledge of high availability configuration.

For hardware and software requirements, see the following guides:

- AppWorks Installation Guide
- AppWorks Platform Installation Guide for Windows
- OpenText Directory Services Installation and Administration Guide

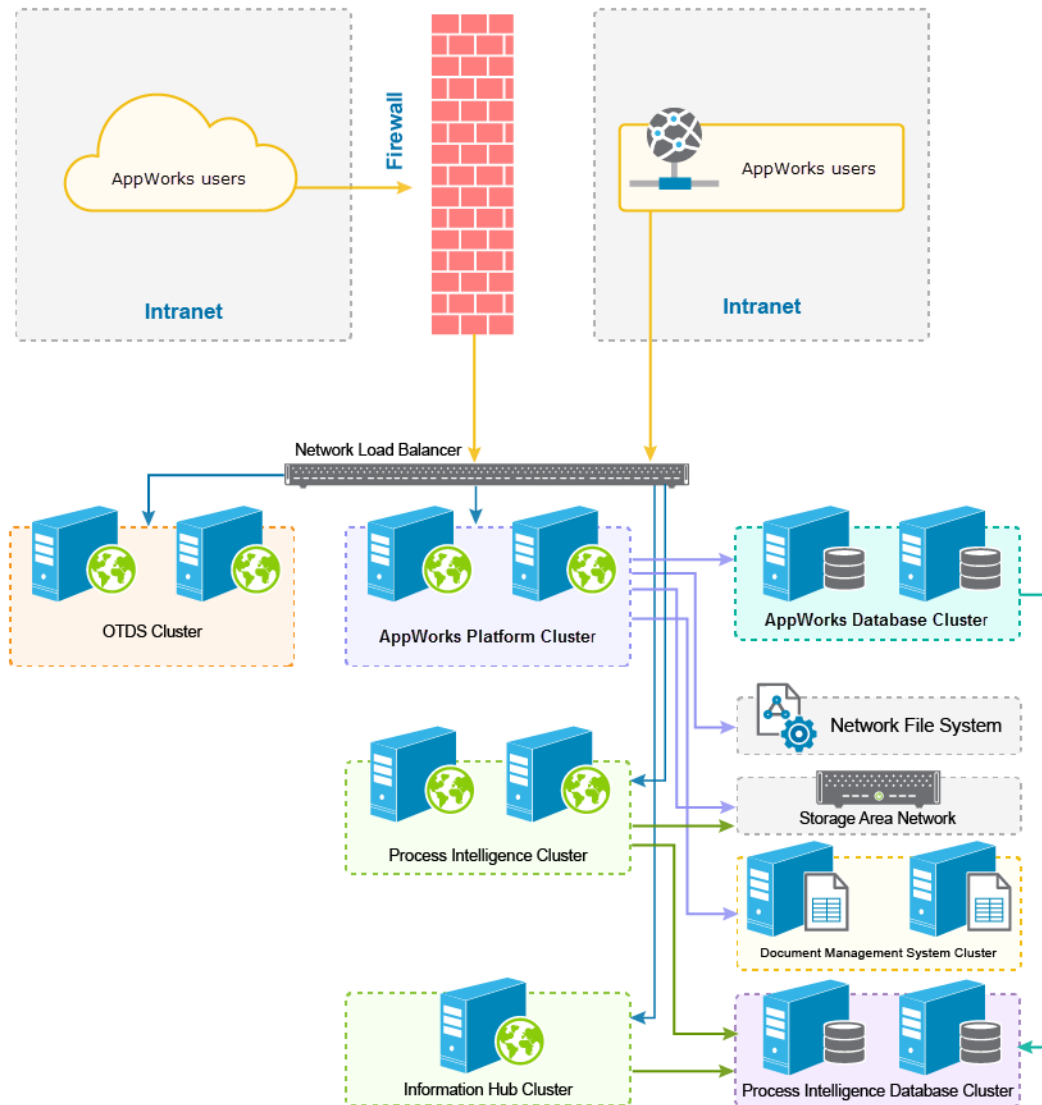
AppWorks high availability architecture

IT infrastructure is a major building block of any enterprise. It comprises various components such as a front-end to validate, send, and receive requests; middleware to process the requests; and a backend to store the information. The arrangement of these elements enables the flow and processing of information, resulting in fulfilling requests.

The IT architectural landscape at a broader level can be categorized into Presentation, Processing, and Persistence tiers. Various software and hardware components can be grouped based on their underlying functionality with these tiers.

AppWorks fits into the Processing tier, as it gives complete control over the internal business processes and serves as a total enterprise application development platform.

The following diagram depicts AppWorks high availability:



The different tiers and the corresponding components can be mapped as follows:

Tier	Objects/Components
Presentation	User Interfaces, Web gateways
Processing	AppWorks
Persistence	Database, File system, Directory Server

After successful configuration, the AppWorks cluster can be accessed in the following ways:

User	Cluster URL
AppWorks Platform admin	<code>http://NLB/home/system</code>
AppWorks Client (formerly Process Experience)	<code>http://NLB/home/system/app/start</code>
OTDS login	<code>http://NLB/otds-login</code>

Note: NLB represents Network Load Balancer.

Identifying high-availability components

Ensuring seamless and uninterrupted communication between interdependent components is vital for any enterprise. Therefore, it is essential to identify the components in the business system that need to be highly available and then to configure them for high availability.

AppWorks products

The following products must be made highly available as they are shipped with AppWorks.

Component	Description	Clustering technologies
AppWorks Platform	Platform that enables organizations to handle complex process automation and case management challenges from a single platform. Provides work-flow capabilities. It includes both modeling and runtime engines, and provides a single and intuitive work experience	<ul style="list-style-type: none"> ■ AppWorks Platform built-in clustering ■ OpenText CARS Master-Master replication ■ Network load balancer ■ Network file system ■ Network load

Component	Description	Clustering technologies
	for users, irrespective of the process engine driving a process on the back end.	
OpenText Process Intelligence	Provides business intelligence data	<ul style="list-style-type: none"> ■ Network Load Balancer ■ Microsoft Cluster (only for Analysis Engine service)
OpenText Directory Services (OTDS)	Facilitates Single Sign-on to work with various components of AppWorks.	<ul style="list-style-type: none"> ■ OTDS Master-Master replication ■ Network Load Balancer

Other components

Depending on the business requirements, the following components may be required to provide high availability:

- Network
- Database systems
- File system
- Network load balancer
- Other backend servers such as the email server, and ERP Systems

Configuring AppWorks high availability

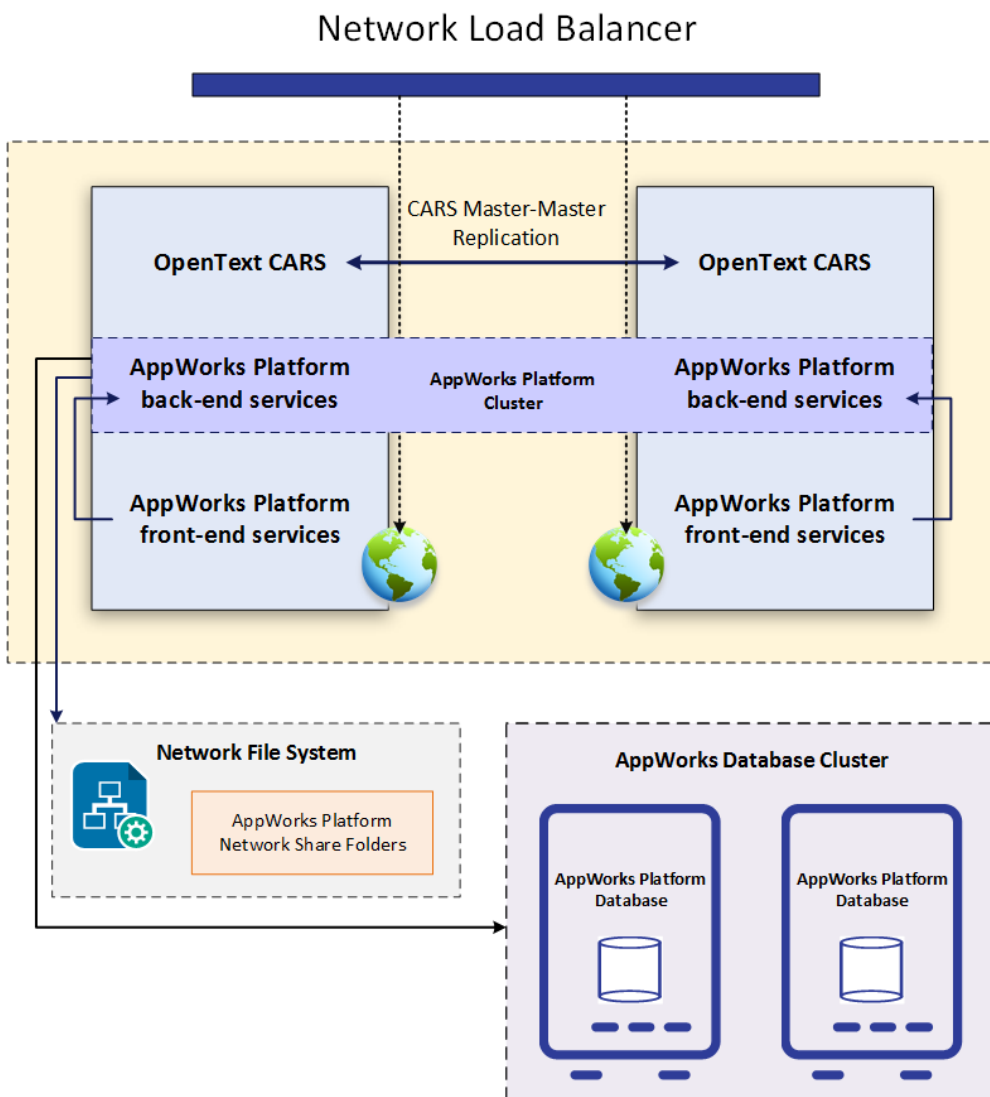
The following products of AppWorks must be highly available:

- OpenText CARS
- AppWorks Platform
- OpenText Process Intelligence
- OpenText Directory Services (OTDS)

Note:

- The following procedure is based on the assumption of a high availability cluster setup with two nodes, referred to as Node1 and Node2.
- Ensure that AppWorks other components are also configured to be in high availability.

The following diagram depicts the high availability cluster consisting of AppWorks Platform and the application:



Configuring AppWorks Platform

To configure AppWorks Platform:

See the above diagram for AppWorks Platform high availability configuration.

1. Install and configure CARS High Availability on Node1 and Node2. See the OpenText CARS section in *AppWorks Platform High Availability Configuration Guide*.

Note: Ensure that the CARS instance name, CARS user name, password, and CARS installation folder structure are identical for both Node1 and Node2.

2. Install and configure AppWorks Platform and service containers high availability on Node1 and Node2, including the application. See the OpenText AppWorks Platform and Service Containers sections in *AppWorks Platform High Availability Configuration Guide*.

Note: Ensure that the AppWorks Platform instance name, Web gateway port, and installation folder structure are identical for Node1 and Node2.

Configuring AppWorks web gateway

To configure AppWorks web gateway:

Note: Ensure that AppWorks Platform is running on both Node1 and Node2 before proceeding.

1. Configure the Network Load Balancer (NLB) for the AppWorks Platform web gateways of Node1 and Node2.
2. Ensure that the Network Load Balancer listening port is identical to the AppWorks Platform web gateway listening port.

HAProxy load balancer example for testing

```
defaults
mode http
retries 3
redispatch
maxconn 2000
contimeout 5000
clitimeout 50000
srvtimeout 50000

listen processsuite 0.0.0.0:8090

balance source
server Node1 10.20.31.183:8090 check inter 500 rise 2 fall 5
server Node2 10.20.31.190:8090 check inter 500 rise 2 fall 5

stats uri /?stats
```

3. Note the Network Load Balancer URL (NLB URL). For example, `http://processsuitecluster:8090/AppWorks Platform`.
4. Add NLB URL to OTDS trusted sites.
5. Modify the connection URL of the OTDS push connector for AppWorks Platform to the AppWorks Platform cluster URL (NLB URL).

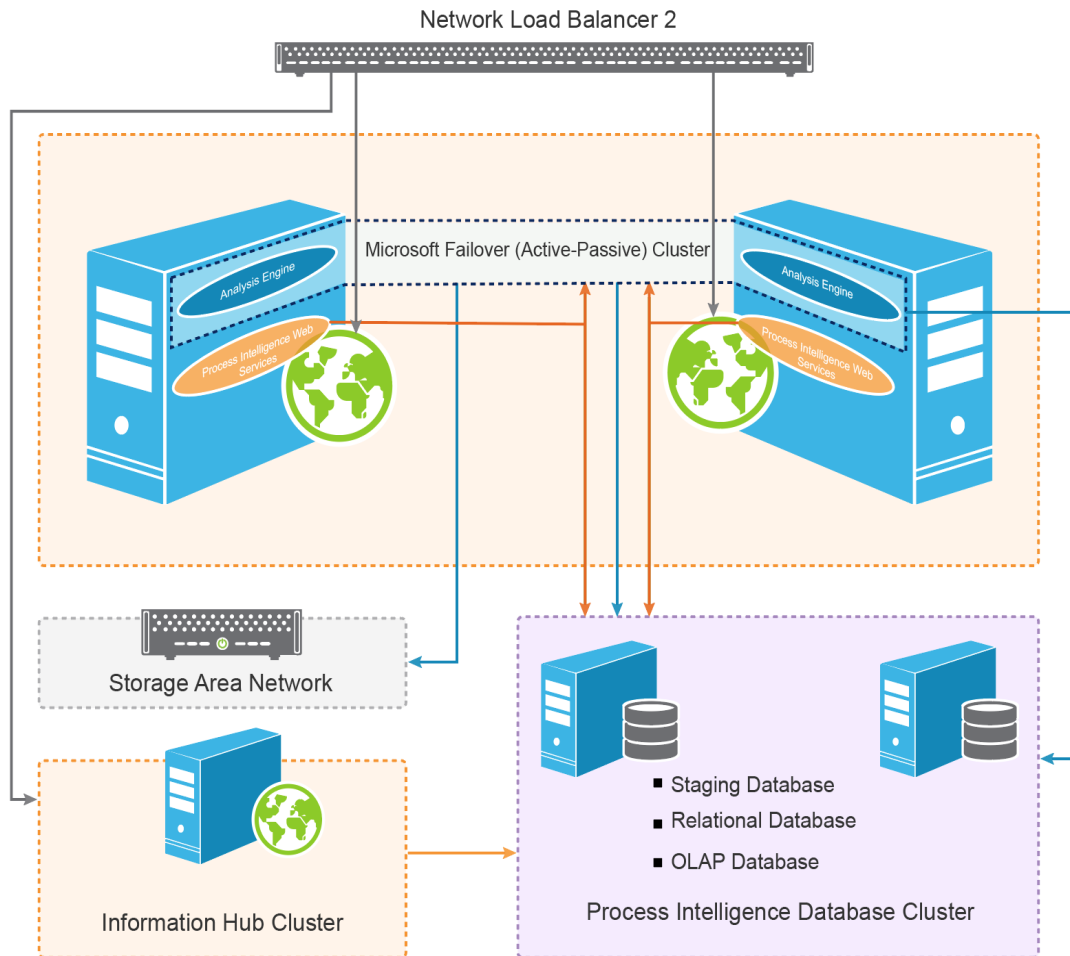
Note:

- The above mentioned network load balancer setting is applicable to all the supported web servers IIS, Apache, and TomEE as these settings are not specific to web servers.

- Since AppWorks Platform and the application are installed on the same cluster, both are installed under the same website. Therefore, no additional steps are required to configure the application in Network Load Balancer.

Configuring Process Intelligence

This section explains how to configure the Process Intelligence high availability cluster.



To configure Process Intelligence:

1. Install Process Intelligence on the first node. See the *Process Intelligence Installation Guide*.
2. Back up the Process Intelligence database.
3. Install Process Intelligence on the second node.
4. Ensure that the Process Intelligence instances on both the nodes point to the same

Process Intelligence database.

5. Configure high availability of various components of Process Intelligence as follows:

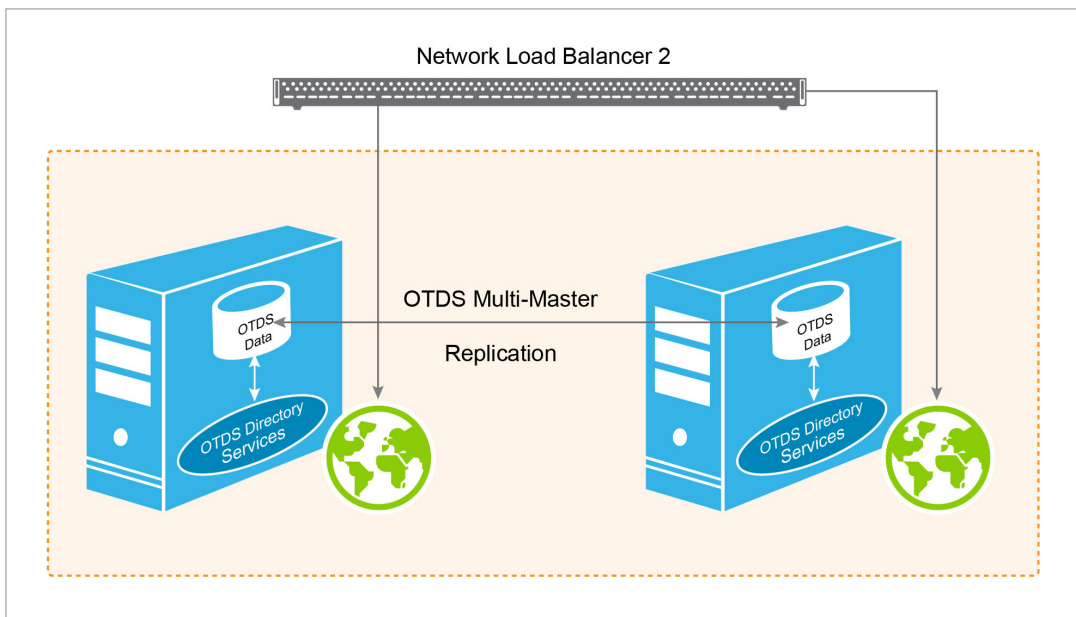
Process Intelligence component	Details	Clustering mechanism	Configuration
Analysis Engine	A Windows Service, that transforms input data from Staging into analytical data in output databases.	Microsoft Failover cluster	Configure the Analysis Engine Windows service with Microsoft Failover cluster. See <i>Microsoft Failover cluster documentation</i> (for example http://technet.microsoft.com/en-us/library/cc732478.aspx).
Integration Web Service	Web service running on IIS.	Network Load Balancer	Configure the corresponding web server with Network Load Balancer.
Relational Staging database	Stores the input data. This database essentially includes a single table called X. The staging which can be populated by external applications. Staging database can be SQL Server or Oracle database.	Database cluster	Depends upon the database.
Relational analytical MS SQL Server database	Database where output data produced by Analysis Engine is written.	Database cluster	Depends upon the database.
OLAP analytical MS SQL Server Analysis Services database	Database where output data produced by Analysis Engine is maintained and ready for reporting.	Database cluster	Depends upon the database.

To uninstall Process Intelligence:

1. Back up the Process Intelligence database.
2. Create a copy of the Process Intelligence database.
3. Configure the current instance of Process Intelligence that must be uninstalled to the Process Intelligence database copy.
4. Uninstall Process Intelligence.

Configuring OpenText Directory Services

To configure the OTDS high availability cluster, see *OpenText Directory Services Installation and Administration Guide* on [My Support](#).



Note: To optimize the hardware, you can configure the OTDS cluster on AppWorks cluster nodes. However, this increases the complexity of the AppWorks cluster and complicates administration.

High availability best practices

The following list provides some general best practices for ensuring a smooth configuration of high availability.

- Ensure that all the nodes in a cluster are set to the identical system time.
- Use nodes with similar hardware and software configurations, as the speed of the slowest node in the high availability cluster affects the efficiency of the clustering.
- Validate the high availability setup before using it in the production environments.

- Do not start cluster nodes simultaneously. There must be a minimum five minute gap between the start up of each node.
- Back up all repositories such as databases, and file systems before performing any modifications to the cluster.

Network file system

Ensure that the network file system you choose supports the following specifications:

- Backup and recovery with required performance.
- Scalability for simultaneous reads and writes from all cluster nodes.
- Highly available hardware device that maintains data.
- High volume data storage that meets business requirements.

Network load balancer

The best practices specific to network load balancers are:

- Hardware-based network load balancers are recommended for better performance and their in-built high availability features.
- Software based load balancers, such as HAProxy, Apache Load Balancer, and Nginx can only be used for testing.
- Check the recommended load balancing algorithm before configuring.

High availability maintenance

To maintain a high availability setup, tasks can involve upgrade or rollback of AppWorks or additional components (operating system, system, and hardware). These tasks revolve around changes in the cluster setup to meet the scaled-up or scaled-down capabilities.

Tasks to maintain a high availability setup:

- Define the policies and strategies for maintenance activities in advance.
- Perform maintenance tasks on nodes in an incremental mode. Do not perform maintenance activities simultaneously on multiple nodes.
- Back up applicable repositories and the complete node before modifying the cluster.
- Ensure that it is possible to roll back at any stage, regardless of the changes in the business system.

Adding a new node to the AppWorks cluster

A growing load of business users demands additional processing capacity. It is a common requirement to add a new AppWorks node to an existing AppWorks cluster.

Adding AppWorks Platform

To add AppWorks Platform on the new node:

1. Install and configure AppWorks Platform on the new node. See the *AppWorks Platform High Availability Configuration Guide*.

Note: Ensure that the AppWorks Platform instance name, AppWorks Platform web gateway port, AppWorks Platform installation folder structure are identical for all nodes.

2. Add the AppWorks Platform web gateway of the new node to the Network Load Balancer (NLB).

Removing a node from AppWorks cluster

Uninstalling AppWorks Platform

To uninstall AppWorks Platform:

1. Back up the AppWorks Platform database and CARS content.
2. Uninstall AppWorks Platform on a given node. See the *AppWorks Platform Installation Guide for Windows*.
3. Remove the corresponding web gateway entry from Network Load Balancer (NLB).

Applying AppWorks updates, fixes, or upgrades

Prerequisites

- Perform maintenance tasks on nodes in an incremental mode. Do not perform maintenance activities simultaneously on multiple nodes.
- Before modifying the cluster, back up the following cluster repositories and file systems:
 - AppWorks Platform LDAP (CARS content)
 - AppWorks Platform database
 - Application database
 - Network File System folders and contents
 - AppWorks Platform installation directory

To apply AppWorks updates, fixes, or upgrades:

1. Follow steps mentioned in the given update or hotfix of AppWorks Platform and the application.
2. Perform the maintenance tasks on all the nodes one after the other. Otherwise the cluster will become inconsistent.

Note: For AppWorks Platform, see the Maintenance section of the *AppWorks Platform High Availability Configuration Guide*.

Validating the high availability configuration

You can validate the AppWorks high availability setup by simulating a situation where the business cases are continuously run against the deployed cluster. The following high availability validation scenarios can be performed on various products involved in the business system.

Note: These scenarios are for validating the high availability of AppWorks products only.

Planned and unplanned outage

- In the planned outage scenario, the administrator intentionally brings down one or more AppWorks products from the production environment. For example, a planned outage can be performed while applying patches, reconfiguring the computer, archiving data, or upgrading the database, application, operating system, or network.
- In the unplanned outage scenario, the administrator abruptly brings down one or more AppWorks products from the existing production environment. For example, an unplanned outage can occur because of human error; software, hardware, and infrastructure failures; site disaster; or natural calamities.

In the following planned and unplanned actions, it is expected that, despite the disruptions, the business use case will continue to run. Once the stopped component is brought online, it will start processing the requests.

Component	Planned outage action	Unplanned outage action
AppWorks Service Containers	Stop the service container. Note: This test case is not applicable to service containers running inside TomEE.	Terminate the Java process corresponding to the service container. Note: This test case is not applicable to service containers running inside TomEE.
OpenText AppWorks Platform (<instance name>)	Stop the OpenText AppWorks Platform (<instance name>).	Terminate the WCP monitor on one of the AppWorks computers, which has at least one active Service Container.
Active LDAP Server (CARS)	Stop the active LDAP server. Note: Ensure that the LDAP service is configured in the Fail-over mode.	Terminate the active LDAP server (CARS).
AppWorks web server	Stop the web server.	Terminate the web server process.
Node restart	Restart one of the AppWorks computers.	

Appendix B

Configuring iHub for AppWorks Platform

Information Hub provides reporting capabilities on the data generated by AppWorks Platform. This enables users analyze the data and present it in the form of reports and dashboards.

Note: Effective with version 16.7, iHub has been renamed to Magellan BI and Reporting.

This topic includes:

1. [Configuring iHub with HTTPS on page 108](#) (Optional)
2. [Configuring system console for iHub on page 109](#)
3. [Deploying Process Suite RSSE on page 110](#)
4. [Configuring AppWorks Platform for iHub on page 112](#)
5. [Integrating Process Intelligence with iHub on page 113](#)

Prerequisites

You must have the following components installed:

- System console
- Information Hub

Note: See the Information Hub Installation, Configuration, and Administration Guide on [My Support](#) for the installation instructions.

Configuring iHub with HTTPS

You can communicate with iHub over both HTTP and HTTPS protocols. While the default configuration is over HTTP, follow these steps to enable the HTTPS communication:

To configure iHub with HTTPS protocol:

1. Open the `<iHub_installldir>\modules\BIRTiHub\iHub\shared\config\acserverconfig.xml` file.

2. Add the following attributes to the `<System>` element:
 - `EnforceSSL="true"`
 - `RSSEIsHTTPS="true"`
3. Open the `<iHub_installdir>\modules\BIRTiHub\iHub\web\birtservice\WEB-INF\volumeProfile.xml` file.
4. Specify the `Server URL` attribute with the protocol and port number, that is `https` and `8001` respectively.
For example: `<ServerUrl>https://<iHub host name>:8001</ServerUrl>`

Note: If port 8001 is not available, open the `<AppWorks Platform_installdir>\config\wcp.properties` file, add the following entries:

 - `ihub.rest.https.port=<relevant port number>`
 - `ihub.portal.https.port=<relevant port number>`
5. Open **Services.msc**, right-click **OpenText iHub <version>**, and select **Restart**.
6. Open the `<iHub_installdir>\modules\BIRTiHub\iHub\etc\acpmdconfig.xml` file.
7. Locate the `samlEntityID` attribute and modify the protocol and port number as shown in the sample below.
`https://<iHub host name>:8701/iportal`
8. Open a browser and type the following URL to verify if the iHub iPortal is running on the HTTPS port:
`https://<iHub host name>:8701/iportal/login.do`

The iHub home page is displayed if the configuration is successful.

Configuring system console for iHub

The system console provides the graphical user interface for configuring, licensing, administering, and monitoring one or more iHub systems. You can create multiple volumes, which can be mapped to organizations in AppWorks Platform.

To configure the system console for iHub:

1. Open a browser and enter `http://<iHub host name>:8500/sysconsole` to sign in to iHub System Console.
2. Type **sysadmin** for the username and password for the user.
3. Click **Clusters** and select **DefaultCluster**.
4. On the DefaultCluster page, click **Add Cluster Node**.
The Add Cluster Node dialog box is displayed.
5. Type the `<iHub host name>` and description for the cluster node, and click **OK**.

System Console is configured for iHub.

Deploying Process Suite RSSE

You must deploy Process Suite Report Server Security Extension (RSSE) on the iHub server to enable communication between AppWorks Platform and iHub. Process Suite RSSE is responsible for handling authentication for requests from AppWorks Platform and direct sign in to the iHub portal.

Single sign on facility through OTDS does not exist between AppWorks Platform and iHub. Therefore, whenever AppWorks Platform communicates with iHub, the Process Suite RSSE running on the iHub server delegates the authentication responsibility to AppWorks Platform for verifying the user credentials.

The Process Suite RSSE driver uses Apache Axis2 libraries and is implemented as an Axis2 Web service. Therefore, it can be deployed on any server that already has Axis2 deployed.

To deploy and configure Process Suite RSSE to the embedded Tomcat for iHub:

1. Navigate to the `<AppWorks Platform_installldir>\components\ihubconnector\authentication` plugin folder.
2. Right-click `axis2.zip` and extract the contents to `<iHub>\modules\BIRTiHub\iHub\web\webapps\`. The `axis2` folder is created and the contents are extracted into that folder.
3. In the `axis2` folder, locate `WEB-INF\services\` and update the `RSSEDriver.properties` file with the following properties:

Property	Description
OTDS_BASE_URL	URL of the base REST API endpoint for OTDS. For example, <code>http://otds.server/otdsws/v1</code>
OTDS_QUERY_USER	General user in the OTDS system that can make queries to search for other objects, such as getting a list of users, groups, or similar information. This user must have adequate privileges to successfully complete the operations that are performed within the RSSE driver, dependent on the individual implementation.
OTDS_QUERY_PASS	Query user password.
IHUB_HOME_FOLDER	Base location for all user home folders. Each user found by RSSE will have a subfolder under this base (current implementation is to use username, that is <code>/home/bob@opentext.com</code>)

Property	Description
PLATFORM_BASE_URL	URL of AppWorks Platform. For example, <protocol>://<AppWorks Platform host name>:<port number>/home

- Open the `<iHub_installalldir>\modules\BIRTiHub\iHub\web\webapps\axis2\WEBINF\conf\axis2.xml` file and replace the `<transportReceiver>` element with the following:

```
<transportReceiver name="http"
class="org.apache.axis2.transport.http.AxisServletListener">
<parameter name="port">8700</parameter>
</transportReceiver>
<transportReceiver name="https"
class="org.apache.axis2.transport.http.AxisServletListener">
<parameter name="port">8701</parameter>
</transportReceiver>
```

Note: This snippet provides the default port numbers of iHub for the `http` and `https` protocols. If you modify the default port numbers, ensure that you provide the applicable port numbers.

- Save the file and exit.
- Sign in to the system console.
- Click **Clusters** and click the required cluster.
The Cluster Configuration page is displayed.
- Click **User Management**.
The user management settings are displayed.
- For Select User Management, select **RSSE SOAP Service**.
The applicable properties are displayed below.
- Ensure that the Search Cache Only check box is clear.
- Enter the following property values:

Property	Description
Server name	iHub host name
Port number	Port number. The default port number for HTTP is 8700 and HTTPS is 8701.
Context path	/axis2/services/ProcessSuiteRSSE
Cache timeout	1440

12. Click **Save**.
13. Open the Cluster Configuration page of the cluster containing this iHub instance.
14. From the **Cluster Status Running** list on the right, select **Stop Cluster**.
The Cluster Status Offline status is displayed.
15. **Optional:** Click **Refresh** if you want to know the status of the cluster.
16. From the **Cluster Status Offline** list on the right, select **Start Cluster**.
The modified changes are now effective.
17. Type `<protocol>://<iHub host name>:<port number>/axis2/services/listServices` to verify if the RSSE service is installed. The Process Suite RSSE service must be displayed.

Note: If OTDS has been configured with iHub, you can sign in to the iHub portal directly with OTDS credentials.

Important: You must restart the iHub service whenever the properties in the RSSE Properties file are modified.

Configuring AppWorks Platform for iHub

After installation, AppWorks Platform automatically deploys the iHub Connector packages. This connector creates a service container called iHub and also provides the iHub Connection Manager. To connect to the correct iHub instance, AppWorks Platform stores the iHub URL using the iHub Connection Manager.

Note: When integrating iHub with OTDS and AppWorks Platform, ensure that the `_NAME_` parameter is set to **otExternalID03** during OTDS resource creation for AppWorks Platform. See [Configuring AppWorks Platform for OTDS authentication on page 61](#).

To configure the iHub integration:

1. Open AppWorks Platform explorer and sign in to the system organization.
The explorer window opens the Welcome page.
2. Click **System Resource Manager**.
The System Resource Manager window displays the service containers list.
3. Right-click the iHub service container and select **Start**.
Optionally, set the startup type to **Automatic** if you want this service container to be started automatically whenever AppWorks Platform restarts.
4. On the AppWorks Platform **Welcome** page, click **iHub Connection Manager**.
5. Type the URL of the iHub server you are connecting to, for example, `<protocol>://<iHub host name>:<port number>`, and type the `<iHub volume name>` you use.
 - For the `http` protocol - use 8700 as the port number
 - For the `https` protocol - use 8701 as the port number

Note: If a new iHub volume has not been created, you can type the Default Volume.

6. Click **Test Connection** on the toolbar.
A notification indicating successful connection is displayed.
7. Close the dialog box and click **Save**.

Note: The iHub Connection Manager configuration performed in the system organization is applicable to all the organizations created in AppWorks Platform. Organization administrators can overwrite this shared configuration based on their organization requirement from the iHub Connection Manager in the target organization.

Integrating Process Intelligence with iHub

OpenText Information Hub (iHub) can connect to the Process Intelligence database to display information through reports and dashboards built in OpenText Analytics Designer. To get started quickly, an Analytics Designer project is provided, which contains dashboards, reports, measures, and hierarchies. The sample dashboards and reports can directly be used with Process Intelligence, but also customized using the available measures and hierarchies.

The Process Intelligence iHub Integration Guide contains details about the sample content and provides instructions for using the Analytics Designer project to build reports and dashboards that connect to the Process Intelligence.

Appendix C

AppWorks Platform REST APIs

Invoking AppWorks Platform REST APIs

To invoke the AppWorks Platform REST APIs:

1. Download the REST Client.
2. Configure the REST Client.
3. Invoke the AppWorks Platform REST APIs.

Downloading REST client

To download the REST client:

1. Open the `OpenTextCordysRESTClient` folder from the location where you extracted the AppWorks zip file.
2. Download the AppWorks Platform REST client, `BPMService.war`, from the AppWorks installer package. This is compatible with the latest version of AppWorks Platform.

Configuring REST Client

To configure the REST Client:

1. Deploy the REST Client file into AppWorks or a web application server, for example Tomcat.
2. Edit the `rest.properties` file at `WEB-INF\classes` to configure the AppWorks Platform instance details as specified below:

- **gatewayUrl**: Type the gateway URL of the AppWorks Platform instance. You must include the organization information in the URL that enables you to access the case models and tasks.

For example:

`https://ps.acme.com/home/org1`

- **SDLGateway.wcp**: Type the WSDL gateway URL.

For example:

```
https://ps.acme.com/home/org1/com.eibus.web.tools.wsdl.WSDLGateway.wcp
```

3. Restart the application server.
The REST Client is configured.


Invoking AppWorks Platform REST APIs

To invoke the AppWorks Platform REST APIs:

1. Authenticate the user details using the LOGIN API.
On successful authentication, a SAML artifact token is generated. This token is required when invoking the REST APIs.
2. Invoke the REST APIs as shown in the following example:

```
var request = new XMLHttpRequest();  
request.open("POST", "https://ps.acme.com:8443/BPMService/v1/login", false );  
request.setRequestHeader("user_id","testew13");  
request.setRequestHeader("password","");  
request.setRequestHeader("Content-Type","text/plain");  
request.send(null);
```

A response is generated.

Note: The response is based on the Content-Type provided in the HTTP Header. See REST APIs in the help () accessible from the shortcut bar on the AppWorks Platform interface for more details.

Appendix D

Configuring IIS

This section describes the procedure to configure IIS on a Windows 2012 computer.

To configure IIS on Windows 2012:

1. Click **Start**, right-click **Computer**, and select **Manage**.
The Server Manager window opens.
2. Select **Add Roles and Features** in the Manage menu.
The Add Roles and Features wizard opens displaying the Before you begin page.
3. Click **Next**.
The Select installation type page appears.
4. Select role-based or feature-based Installation and click **Next**.
The Select destination server page appears.
5. Select the appropriate server to configure and click **Next**.
The Select server role page appears.
6. Select Web Server (IIS) and click **Next** until you progress to Role Services configuration.
The Select role services page appears.
7. In the Role Services box, verify if the following features are installed. If they are not installed, select the applicable features and click **Install**.
 - Management Tools
 - IIS 6 Management Compatibility – All options
 - Application Development (Features)
 - Security
 - Basic Authentication
 - Windows Authentication

The required features for IIS are configured.

Appendix E

Upgrading AppWorks

Before you begin:

- BPM Everywhere has been deprecated and is no longer part of AppWorks. Hence, installation or upgrade to the later versions is not supported.
- AppWorks 10.8 and later versions do not support OLEDB. It supports only JDBC.

To upgrade AppWorks:

1. Navigate to the <extracted_installdir> and double-click **Mastersetup.exe**.
2. Based on the products selected, the Mastersetup wizard invokes the corresponding product installers.

The following sections provide references to upgrading various AppWorks components.

Upgrading AppWorks Platform

For upgrading AppWorks Platform instructions, see *AppWorks Platform Upgrade Guide* on [My Support](#).

Upgrading OTDS

For upgrading OTDS instructions, see *OpenText Directory Services Installation and Administration Guide* on [My Support](#)

Upgrading Process Intelligence

Upgrading Process intelligence comprises the following steps:

1. Upgrading Process Intelligence Server
2. Updating the data replication configuration

To upgrade Process Intelligence Server:

See Maintaining the Process Intelligence Server topic in the *Process Intelligence Installation Guide* on [My Support](#).

After completing the upgrade process, if there are any changes to the publisher articles or AEDB database scripts, you must update your existing data replication configuration as specified below:

To update the data replication configuration:

1. Access SQL Server Management Studio, expand **Replication > Local Publication**, right-click the required publication, and select **Properties**.
The Publication properties window opens.
2. Select **Articles** from the Select a Page list.
The Objects to Publish section displays the list of configured tables.
3. Select or clear the check boxes to add or delete tables to the existing configuration.
4. Expand the tables and select or clear the check boxes to add or delete columns from the configured tables.
5. Click **OK**.
The Reinitialize Subscriptions window opens.
6. Click **Mark For Reinitialization**.
The Reinitialize Subscriptions window closes.
7. Access SQL Server Management Studio, expand **Replication > Local Subscription**, right-click the required subscription, and then select **View synchronization Status**.
The View Synchronization Status window opens.
8. When the View Synchronization Status window closes, access the AEDB database to verify if the tables or columns have been updated.

Upgrading Brava

To upgrade Brava:

1. Uninstall existing Brava installation.
2. Install the latest version of Brava. See [Installing and configuring Brava on page 92](#) for the installation instructions.


Appendix F

Troubleshooting

General troubleshooting

Following are a few questions and answers that can help you troubleshoot problems that may occur.

What is the general recommended approach for User Management?

Open Text recommends that you use the OTDS for user management. Configure OTDS Push connectors to synchronize users, groups, and membership to AppWorks Platform. Use the OTDS Push roles functionality available in Security Administration to synchronize the functional roles from AppWorks Platform into OTDS. See the 'Configuring OTDS Push Connector for OpenText CARS and Identity components' topic in the help () accessible from the shortcut bar on the AppWorks Platform interface and the 'Synchronizing roles from AppWorks Platform to OTDS' topic in the *AppWorks Platform Administration Guide*.

What should I do if I get access denied errors?

If the following error occurs:

Access is denied for the Web service operation.

Access is denied for the Web service operation `GetToDoListItems`.

Access denied on Initiation of Process: `prcCaseManagement` for user `userid`.

The probable cause is that the user is not assigned the required roles to perform the operation. Also, the users and roles must be available in AppWorks Platform and OTDS as required. Verify if the users and roles are synchronized correctly.

Troubleshooting OTDS

Following are a few questions and answers that can help you troubleshoot some OTDS problems that may occur.

I have allocated users and groups to my resources, but they do not appear to be in my application. Why not?

Ensure that the resource is configured correctly to synchronize with the application.

Select the OTDS Activity Feed for any errors when attempting to push updates to your application.

Ensure that the users, groups, and user partitions are associated with an access role that is associated with the resource.

Review the OTDS log `directory-access.log` for failure messages. If you have an error Authentication failure `[MULTIPLE_IDENTITIES_FOR_USER_NAME]`, you will have two accounts in different partitions with the same sign in name as you are using for the resources synchronization configuration. You will have to remove one of these users.

Review the OTDS log `directory-provenance.log` for any failure messages that appear related.

Why don't my roles and role members appear in my application?

If you are seeing users in the application, the resource synchronization appears to be working. Check that the access role with the associated groups is marked to Include Groups from Organizational Users.

AppWorks Platform will also interpret a role with a period in the group ID as a AppWorks Platform package role that will match the role created as a part of a AppWorks Platform solution. It is recommended not to include a period in the group ID for other roles being sent to AppWorks Platform.

I have added additional AppWorks Platform solutions with roles, but I do not see the roles in OTDS, why not?

AppWorks Platform does not dynamically create new roles in OTDS for you. Use the OTDS Push roles functionality available in Security Administration. For more information, see the Synchronizing roles from *AppWorks Platform* to OTDS topic in the *AppWorks Platform Administration Guide*.

I have created my custom roles in OTDS as groups, but anyone I have associated with the group does not appear in AppWorks Platform, what has gone wrong?

Ensure that the resource is configured to synchronize to the application, and that the configuration is correct.

Review the OTDS Activity Feed for any errors when attempting to push updates to your application.

Be sure that there are no spelling mistakes in the group in OTDS for the Group ID, and that the Group ID reflects the package name followed by a period and then the name with no additional spaces.

I experienced some errors during a resource synchronization operation and now some users or group membership information may not have reached my applications, how do I resubmit the changes?

You cannot resubmit the changes themselves, but you can request a consolidate operation on the user partition, user, or group which will force that object and its components to be resubmitted to the application for synchronization. It is not recommended to do this frequently as this may take a long time to complete depending on the size of the user partition or group.

Note: This does not re-submit any deletion notifications so a user that was removed from OTDS or your enterprise user store may still exist in the application user store. Because OTDS is performing the authentication requests, even though the user will remain in the products user store, that user would not be able to get access to the system.

Are the AppWorks Platform User Management Connector or low level LDAP Connector supported with OTDS?

AppWorks Platform enables applications to create roles through the User Management Connector as well as the low level LDAP Connector. These Connectors are not adapted to work with OTDS and the AppWorks Platform User tools are supported when AppWorks Platform is installed and used without the rest of AppWorks and OTDS for authentication and user management.

How do I manage my OTDS environment?

Two clients are available to manage your OTDS environment.

- The Administration Client, an MMC-based client that is installed on an administrator computer and configured to point to OTDS.
- Web Administration Client, introduced in OTDS 10.5 SP1, enables you to maintain your OTDS environment from a web browser. The Web Administration client is installed as part of the application.

Appendix G

Configuring online help on a Private Help Server

Providing the online help on a local help server (Private Help Server)

The online help for this product is delivered using the OpenText Global Help Server (GHS) system, which provides your users with live access to the latest version of the help. If you cannot use the GHS system (for example, if your site does not have Internet access), you can install the OpenText Private Help Server (PHS), a local version of the help system that can host your OpenText product online help on your organization's network. After the PHS is installed, you can then configure your OpenText product(s) to forward all online help requests to your PHS.

For detailed information about installing the PHS, see *OpenText™ Help System - Private Help Server Administration Guide (OTHS-AGD)*.

Note:

- The Private Help Server can support multiple OpenText products. If the Private Help Server has already been installed within your organization to support another OpenText product, you can add additional OpenText product online helps to that installation.
- If you are replacing a previous PHS installation, see *OpenText™ Help System - Private Help Server Administration Guide (OTHS-AGD)*.
- If the server you want to use for the PHS installation cannot connect to the Internet, see *OpenText™ Help System - Private Help Server Administration Guide (OTHS-AGD)*.
- If you want to use Apache TomEE as the web server, while installing PHS for AppWorks Platform, you can provide TomEE details in sections that require web server details.

After the PHS is installed or upgraded, you can use its Online Help Deployer to download online helps from the GHS system by entering the deployment code(s) listed in the table below. For more information about using the codes, see *OpenText™ Help System - Private Help Server Administration Guide (OTHS-AGD)*.

Code	Product
otags-167-help	OpenText AppWorks Platform documentation

Configuring AppWorks Platform to use a local help server (Private Help Server)

After you install a PHS and deploy the OpenText AppWorks Platform online help, you must redirect help requests to it.

To redirect help requests:

After all the guides are deployed, you must configure the PHS URL in AppWorks Platform. If you have multiple organizations, the following steps must be performed in all the organizations individually.

1. Open AppWorks Platform explorer and click **XML Store Explorer**.
2. Navigate to /Cordys/WCP/Desktop/CUSPShortcuts/documentation.
3. For the url node, enter `http://<FQDN>:<web server port number>/OTHelpServer/mapper/`
For example:
`<url>http://myhelpserver.opentext.net:81/OTHelpServer/mapper</url>`
4. Click **Save**.
5. Refresh the browser.
6. Click the documentation icon in the shortcuts panel of the application.

The landing page of the AppWorks Platform online help opens.